Avaya Solution & Interoperability Test Lab

Application Notes for Configuring COLT SIP Trunking with Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2.1 using TLS – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between COLT SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager 6.3, Avaya Session Border Controller for Enterprise 6.2.1 Q18 and various Avaya endpoints.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as the observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

COLT is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between COLT SIP Trunking and an Avaya SIP-enabled enterprise solution using TLS/SRTP. The Avaya solution consists of Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager 6.3, Avaya Session Border Controller for Enterprise (Avaya SBCE) 6.2.1 Q18 and various Avaya endpoints, listed in **Section 4**.

Customers using this Avaya SIP-enabled enterprise solution with COLT SIP Trunking are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to COLT SIP Trunking via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and the Avaya SBCE with various types of Avaya phones.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test.

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from softphones. Two Avaya softphones were used in testing: Avaya one-X® Communicator and Avaya Flare® Experience for Windows. Avaya one-X® Communicator supports two work modes (Computer mode). Each supported mode was tested. Avaya one-X® Communicator also supports two Voice over IP (VoIP) protocols: H.323 and SIP. Both protocols were tested. Avaya Flare® Experience for Windows was used in testing as a simple SIP endpoint for basic inbound/outbound calls.
- SIP transport using TLS as supported.

- Direct IP-to-IP Media (also known as “Shuffling”) over a SIP Trunk. Direct IP-to-IP Media allows Communication Manager to reconfigure the RTP path after call establishment directly between the Avaya phones and the Avaya SBCE releasing media processing resources on the Avaya Media Gateway.
- Various call types including: local, long distance, international, outbound toll-free.
- Codec G729, G.711A.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call transfer, conference, off-net call forwarding, forwarding to Avaya Aura® Messaging and EC500 mobility (extension to cellular).
- Use SIP RE-INVITE for call transfer.
- Use Diversion Header for call forward.
- Call Center scenarios.
- Fax T.38.

Items not supported or not tested included the following:

- Inbound toll-free, operator-assisted, local directory assistance, and emergency calls were not tested because these services were not available during the compliance test.
- COLT system does not support Registration and Authentication.

2.2. Test Results

The objectives outlined in **Section 2.1** were verified. Interoperability testing of COLT SIP Trunking was completed with successful results for all test cases.

2.3. Support

For technical support on the COLT system, please use the support link at http://www.colt.net/uk/en/enterprise/index.htm , or call the customer support number at +44 203 140 2185.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to COLT SIP Trunking. This is the configuration used for compliance testing.

For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

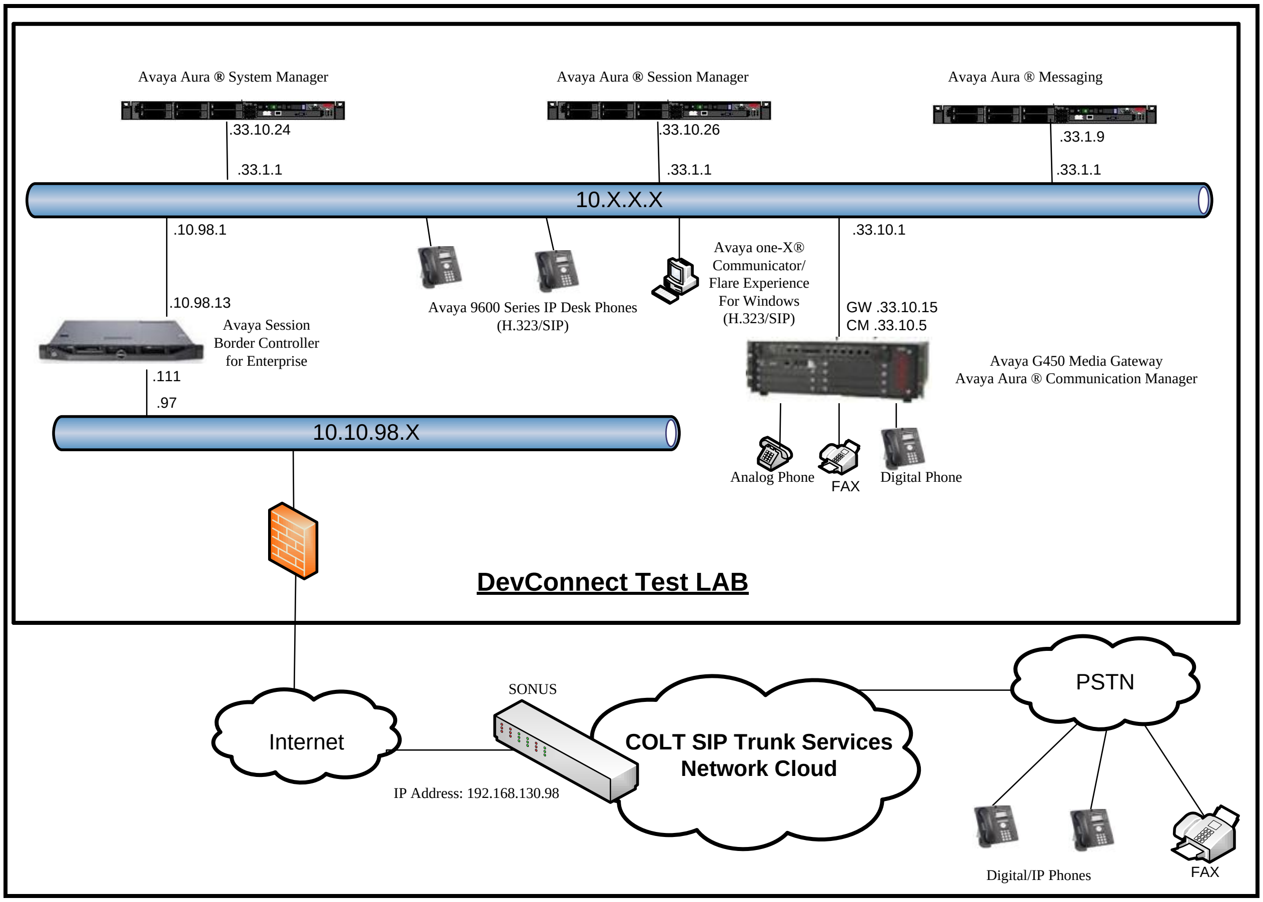

Avaya Aura ® System Manager
Avaya Aura ® Session Manager
Avaya Aura ® Messaging
.33.10.24
.33.10.26
.33.1.9
.33.1.1
.33.1.1
.33.1.1
10.X.X.X
.10.98.1
.33.10.1
Avaya one-X® Communicator/ Flare Experience For Windows (H.323/SIP)
.10.98.13
Avaya 9600 Series IP Desk Phones (H.323/SIP)
GW .33.10.15
CM .33.10.5
Avaya Session Border Controller for Enterprise
Avaya G450 Media Gateway
Avaya Aura ® Communication Manager
.111
.97
10.10.98.X
Analog Phone
FAX
Digital Phone
DevConnect Test LAB
SONUS
PSTN
Internet
COLT SIP Trunk Services Network Cloud
IP Address: 192.168.130.98
Digital/IP Phones
FAX

Figure 1: Avaya IP Telephony Network and COLT SIP Trunking

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Avaya IP Telephony Solution Components	
Equipment/Software	**Release/Version**
Avaya Aura® Communication Manager running on Avaya S8300 Server	6.3.6 (R016x.03.0.124.0- 21591)
Avaya G450 Media Gateway – MM711AP Analog – MM712AP Digital – MM710AP	 HW46 FW096 HW10 FW014 HW05 FW020
Avaya Aura® Session Manager running on Avaya S8800 Server	6.3.7 (6.3.7.0.637008)
Avaya Aura® System Manager running on Avaya S8800 Server	6.3.9 (Build No. - 6.3.0.8.5682 - 6.3.8.4417) (Software Update Revision No: 6.3.9.1.2538)
Avaya Aura® Messaging running on Avaya S8800 Server	6.2 SP2
Avaya Session Border Controller for Enterprise running on Dell R210 V2 Server	6.2.1 Q18
Avaya 9630 IP Deskphone (SIP)	Avaya one-X® Deskphone SIP Edition 2.6.6.0
Avaya 9640 IP Deskphone (H.323)	Avaya one-X® Deskphone Edition 3.2
Avaya 9630 IP Deskphone (H.323)	Avaya one-X® Deskphone Edition 3.2
Avaya Flare® Experience for Windows	1.1.4.23
Avaya one-X® Communicator (H.323 & SIP)	6.1.9.04 SP9-132
Avaya Digital Telephones (1408D)	N/A
Nortel Symphony 2000 Analog telephone	N/A
HP Officejet 4500 Fax	N/A
COLT SIP Trunking Components	
Equipment/Software	**Release/Version**
SONUS	8.4.11

Table 1: Equipment and Software Tested

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya servers and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

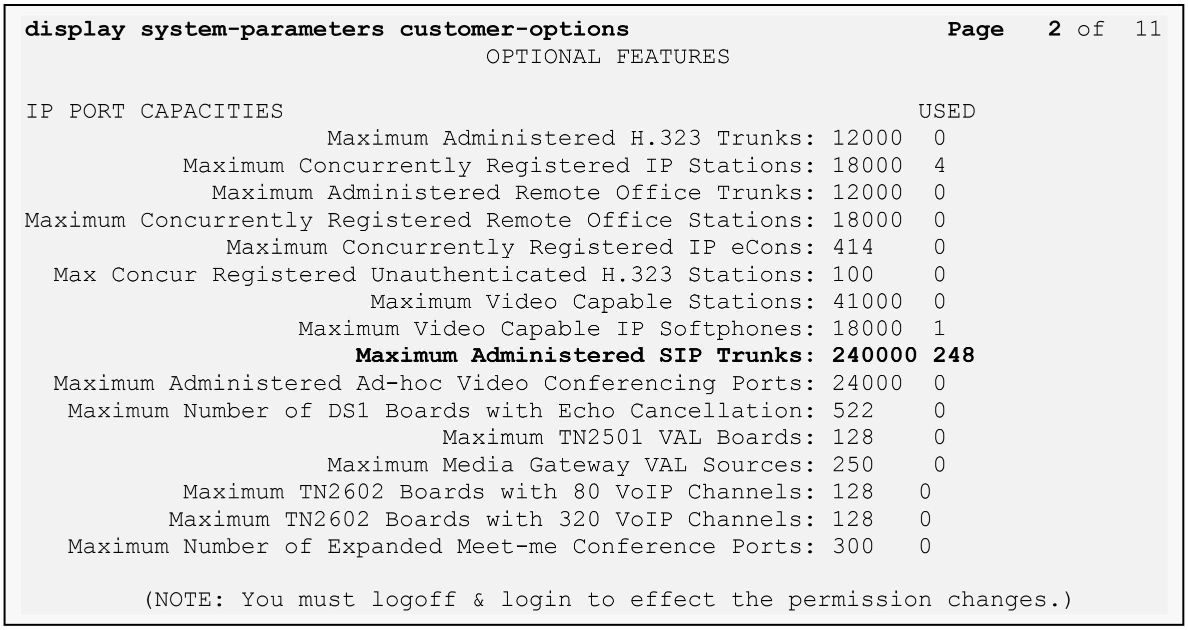
5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for COLT SIP Trunking. It is assumed the general installation of Communication Manager, Avaya Media Gateway and Session Manager has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that **24000** SIP trunks are available and **248** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.



```
display system-parameters customer-options                      Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 12000  0
           Maximum Concurrently Registered IP Stations: 18000  4
             Maximum Administered Remote Office Trunks: 12000  0
Maximum Concurrently Registered Remote Office Stations: 18000  0
              Maximum Concurrently Registered IP eCons: 414    0
  Max Concur Registered Unauthenticated H.323 Stations: 100    0
                        Maximum Video Capable Stations: 41000  0
                   Maximum Video Capable IP Softphones: 18000  1
                       Maximum Administered SIP Trunks: 240000 248
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 522    0
                             Maximum TN2501 VAL Boards: 128    0
                     Maximum Media Gateway VAL Sources: 250    0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

        (NOTE: You must logoff & login to effect the permission changes.)
```

Figure 2: System-Parameters Customer-Options Form – Page 2

On **Page 3**, verify that **ARS** is set to **y**.

```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? n           Audible Message Waiting? y
        Access Security Gateway (ASG)? n               Authorization Codes? n
        Analog Trunk Incoming Call ID? n                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? n                          CAS Main? n
Answer Supervision by Call Classifier? n                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? n
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? y
          ASAI Link Core Capabilities? y                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? y                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n     Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? y
                                 ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

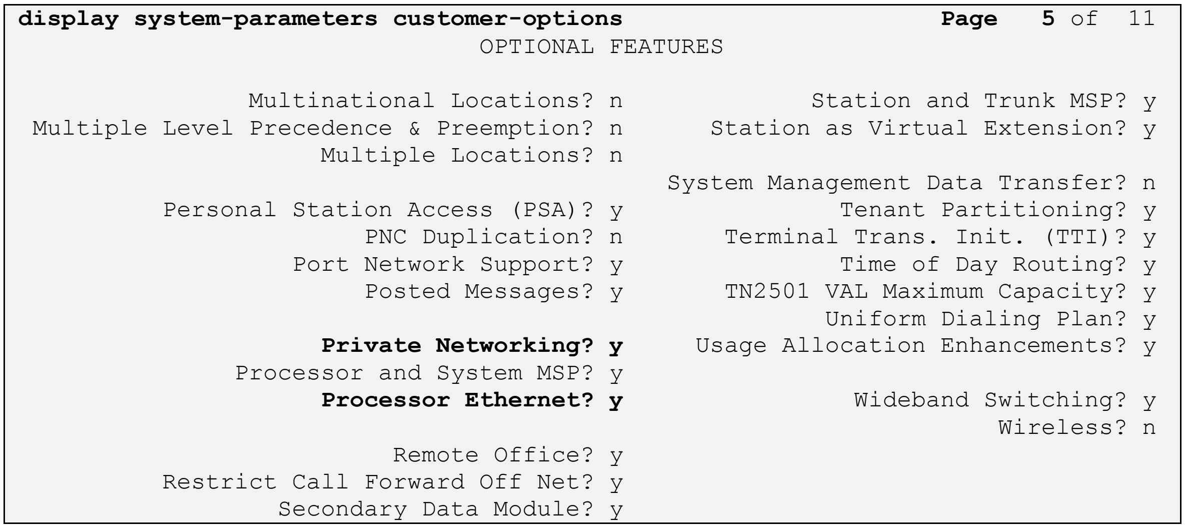
Figure 3: System-Parameters Customer-Options Form – Page 3

On **Page 4**, verify that **IP Trunks** field is set to **y** and **Media Encryption Over IP** field is set to **y**.
(Note: The Media Encryption option is only available if **Media Encryption Over IP** is enabled on the installed license).

```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                                IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                          ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                            ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                   ISDN-PRI? y
              ESS Administration? y               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                     Malicious Call Trace? y
     External Device Alarm Admin? y                 Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                   Multifrequency Signaling? y
      Global Call Classification? y           Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y        Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y                Multimedia IP SIP Trunking? y
                       IP Trunks? y

           IP Attendant Consoles? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

Figure 4: System-Parameters Customer-Options Form – Page 4

On **Page 5**, verify that **Private Networking** and **Processor Ethernet** are set to **y**.

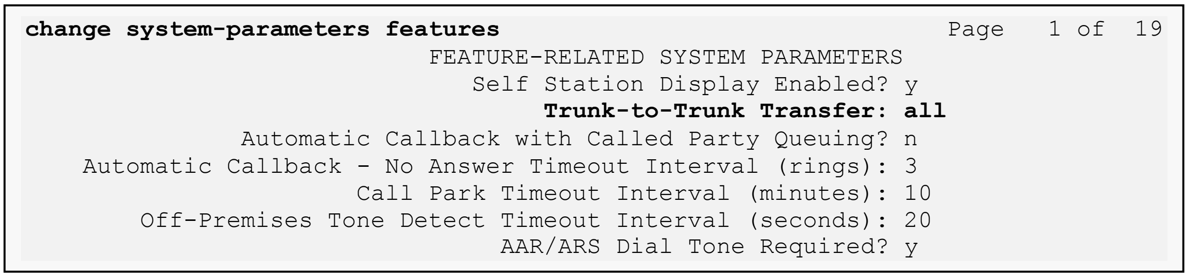


```
display system-parameters customer-options                      Page   5 of  11
                                OPTIONAL FEATURES

                Multinational Locations? n             Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? n      Station as Virtual Extension? y
                     Multiple Locations? n
                                            System Management Data Transfer? n
          Personal Station Access (PSA)? y               Tenant Partitioning? y
                        PNC Duplication? n       Terminal Trans. Init. (TTI)? y
                   Port Network Support? y               Time of Day Routing? y
                        Posted Messages? y       TN2501 VAL Maximum Capacity? y
                                                        Uniform Dialing Plan? y
                     Private Networking? y     Usage Allocation Enhancements? y
               Processor and System MSP? y
                     Processor Ethernet? y                Wideband Switching? y
                                                                    Wireless? n
                          Remote Office? y
          Restrict Call Forward Off Net? y
                  Secondary Data Module? y
```

Figure 5: System-Parameters Customer-Options Form – Page 5

5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** for allowing inbound calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to be transferred back to the PSTN then leave the field set to **none**.



```
change system-parameters features                               Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
```

Figure 6: System-Parameters Features Form – Page 1

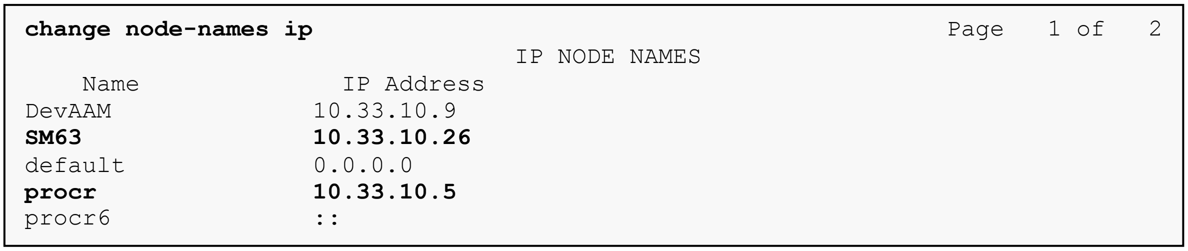
On **Page 9**, verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **anonymous** for both.

```
change system-parameters features                               Page   9 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: anonymous
  CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous

DISPLAY TEXT
                                       Identity When Bridging: principal
                                        User Guidance Display? n
 Extension only label for Team button on 96xx H.323 terminals? n

INTERNATIONAL CALL ROUTING PARAMETERS
                 Local Country Code: 1
          International Access Code: 011

SCCAN PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

CALLER ID ON CALL WAITING PARAMETERS
     Caller ID on Call Waiting Delay Timer (msec): 200
```

Figure 7: System-Parameters Features Form – Page 9

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager **(procr**) and Session Manager (**SM63**). These node names will be needed for defining the service provider signaling group in **Section 5.7**.

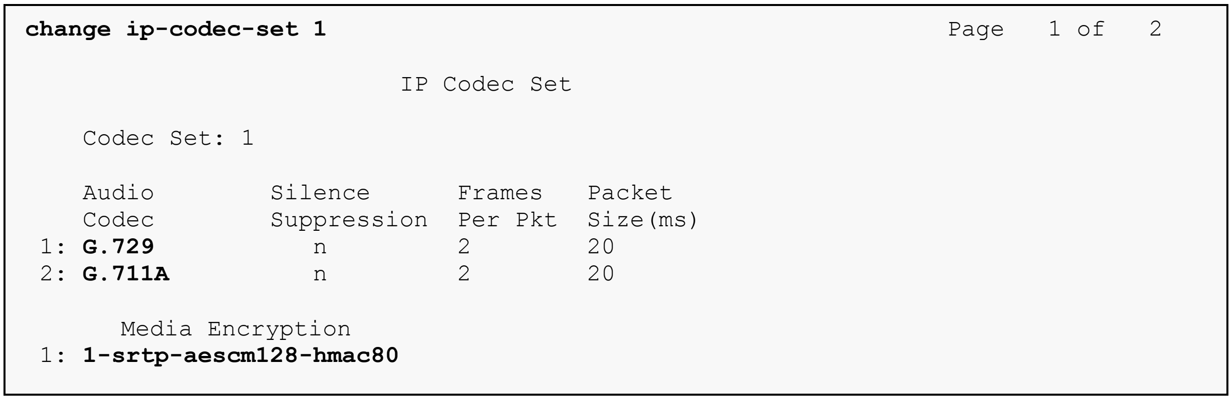


```
change node-names ip                                             Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
DevAAM              10.33.10.9
SM63                10.33.10.26
default             0.0.0.0
procr               10.33.10.5
procr6              ::
```

Figure 8: Node-Names IP Form

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 1 was used for this purpose. COLT SIP Trunking supports the **G.729** and **G.711A** codecs and **srtp-aescm128-hmac80** unencrypted_SRTCP for media encryption. Default values can be used for all other fields.



```
change ip-codec-set 1                                            Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.729           n         2        20
 2: G.711A          n         2        20

      Media Encryption
 1: 1-srtp-aescm128-hmac80
```

Figure 9: IP-Codec-Set Form – Page 1

On **Page 2**, to enable fax t.38, set the **Fax Mode** to **t.38-standard**. Otherwise, set the Fax Mode to **off**.

```
change ip-codec-set 1                                          Page   2 of   2

                          IP CODEC SET

                              Allow Direct-IP Multimedia? n



                         Mode                Redundancy              Packet Size(ms)
    FAX                  t.38-standard        1           ECM: y
    Modem                off                  0
    TDD/TTY              US                   3
    H.323 Clear-channel  n                    0
    SIP 64K Data         n                    0                       20
```

Figure 10: IP-Codec-Set Form – Page 2

5.5. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP network region **1** was chosen for the service provider trunk. Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **bvwdev7.com**. This name appears in the From header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes.** Shuffling can be further restricted at the trunk level on the Signaling Group form (**Session 0**).
- Set the **Codec Set** field to the IP codec set defined in **Section 0**.
- Default values can be used for all other fields.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1         Authoritative Domain: bvwdev7.com
    Name: procr                      Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Figure 11: IP-Network-Region Form

5.6. Configure IP Interface for procr

Use the **change ip-interface procr** command to change the Processor Ethernet (procr) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the procr for SIP Trunk signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones. Ensure **Enable Interface** is **y** and **Network Region** is **1**.

```
change ip-interface procr
                                  IP INTERFACES

                  Type: PROCR
                                                       Target socket load: 19660

      Enable Interface? y                           Allow H.323 Endpoints? y
                                                     Allow H.248 Gateways? y
        Network Region: 1                             Gatekeeper Priority: 5

                                 IPV4 PARAMETERS
             Node Name: procr                   IP Address: 10.33.10.5
           Subnet Mask: /24
```

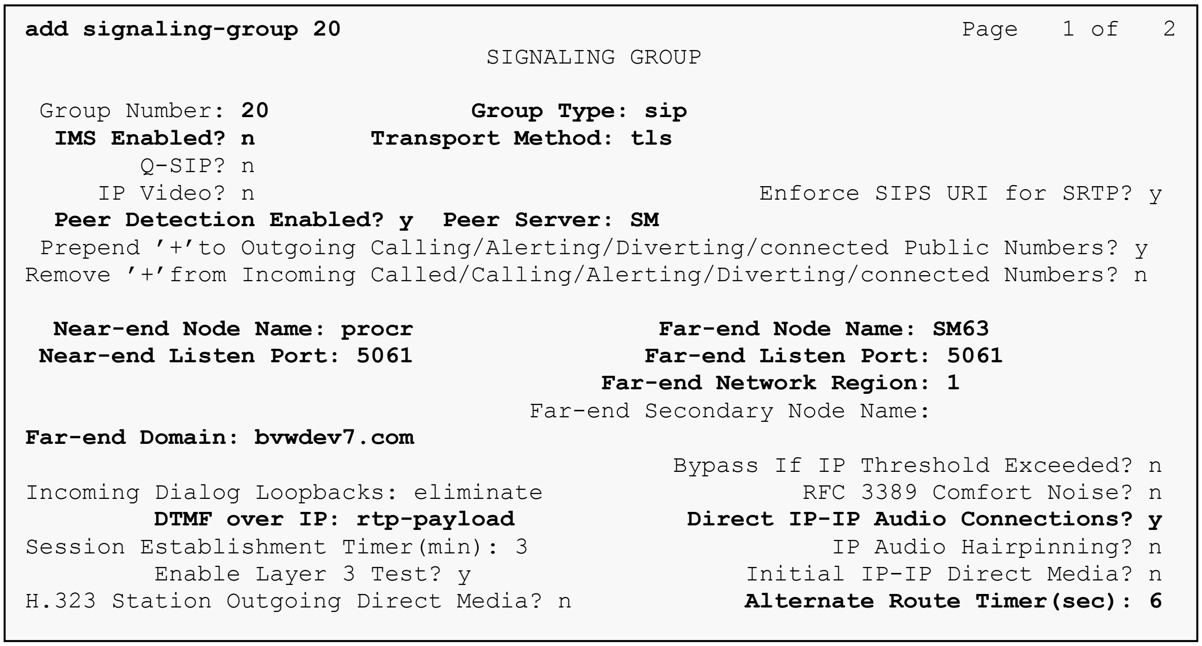
Figure 12: IP-Interface Form

5.7. Signaling Group

Use the **add signaling-group** command to create signaling groups between Communication Manager and Session Manager. The signaling group is used for both inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group **20** was used for outbound and inbound calls. It was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the value of **tls** (Transport Layer Security). The transport method specified here is used between Communication Manager and Session Manager.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SM63**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid used port for TLS as **5061**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 0**.

- Set the **Far-end Domain** to **bvwdev7.com** of the enterprise domain.
- Set **Direct IP-IP Audio Connections** to **y**. This setting will enable media shuffling on the SIP trunk so that Communication Manager will redirect media traffic directly between the SIP trunk and the enterprise endpoint. Note that Avaya Media Gateway will not remain in the media path of all calls between the SIP trunk and the endpoint.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to **6**. This defines the number of seconds the Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.



```
add signaling-group 20                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 20             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+'to Outgoing Calling/Alerting/Diverting/connected Public Numbers? y
Remove '+'from Incoming Called/Calling/Alerting/Diverting/connected Numbers? n

  Near-end Node Name: procr                   Far-end Node Name: SM63
 Near-end Listen Port: 5061                  Far-end Listen Port: 5061
                                          Far-end Network Region: 1
                                   Far-end Secondary Node Name:
Far-end Domain: bvwdev7.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

Figure 13: Signaling-Group Form

5.8. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 0**. For the compliance test, trunk group **20** was used for outbound and inbound calls. It was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field. (i.e**. *020**).
- Set **Direction** to **two-way**.
- Set the **Service Type** field to **public-ntwrk**.

- Set **Member Assignment Method** to **auto**.
- Set the **Signaling Group** to the signaling group configured in **Section 0**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
add trunk-group 20                                                Page   1 of  21
                                TRUNK GROUP

Group Number: 20                    Group Type: sip          CDR Reports: y
Group Name: SIP Trunks                   COR: 1        TN: 1        TAC: *020
   Direction: Two-way           Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 20
                                                     Number of Members: 10
```

Figure 14: Trunk-Group Form – Page 1

On **Page 2**, set the **Redirect On OPTIM Failure** timer to the same amount of time as the **Alternate Route Timer** on the signaling group form in **Section 0**. Note that the **Redirect On OPTIM Failure** timer is defined in milliseconds. Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

```
add trunk-group 20                                                Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 6000

            SCCAN? n                                 Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval (sec): 600
Disconnect Supervision -   In? y   Out? y

             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

Figure 15: Trunk-Group Form – Page 2

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers. The compliance test used 12 digits in numbering format. Thus, **Numbering Format** was set to **private** and the **Numbering Format** field in the route pattern was set to **unk-unk** (see **Section 5.10**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 0** if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if an enterprise user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```
add trunk-group 20                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y



                                Modify Tandem Calling Number: no


 Show ANSWERED BY on Display? y
```

Figure 16: Trunk-Group Form – Page 3

On **Page 4**, the **Network Call Redirection** field can be set to **n** (default setting) so that the SIP REFER is not sent. Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** and **Support Request History** fields provide additional information to the network if the call has been re-directed. These settings are needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set the **Telephone Event Payload Type** to **101**.

```
add trunk-group 20                                                  Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n
          Build Refer-To URI of REFER From Contact For NCR? n
                                     Send Diversion Header? y
                                   Support Request History? n
                              Telephone Event Payload Type: 101

                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
```

Figure 17: Trunk-Group Form – Page 4

5.9. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since private numbering was selected to define the format of this number (**Section 0**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the SIP service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs). It is used to authenticate the caller.

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single private-numbering entry can be applied for all extensions. In the example below, all stations with a 4-digit extension beginning with **005** will send the calling party number as the **Private Prefix** plus the extension number.

```
change private-numbering 0                                    Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 4  005              20         44207190         12     Total Administered: 7
                                                         Maximum Entries: 540
```

Figure 18: Private-Numbering Form

5.10. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit **9** is used as the ARS access code. Enterprise callers will dial **9** to reach an “outside line”. This common configuration is illustrated below. Use the **change dialplan analysis** command to define a **Dialed String** beginning with **9** of **Length 1** as a feature access code (**fac**).

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 2

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type

   005         4    ext
   11          4    ext
   18          4    ext
   9           1    fac
   *           4    dac
   #           4    dac
```

Figure 19: Dialplan Analysis Form

Use the **change feature-access-codes** command to configure **9** as the **Auto Route Selection (ARS) – Access Code 1**.

```
change feature-access-codes                                     Page   1 of  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialin3g List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *111
                       Answer Back Access Code:
                         Attendant Access code:
      Auto Alternate Routing (AAR) Access Code: *100
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:     Deactivation:
Call Forwarding Activation Busy/DA:        All:     Deactivation:
   Call Forwarding Enhanced Status:        Act:     Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:        Close Code:
```

Figure 20: Feature–Access-Codes Form

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit **9**. The example below shows a subset of the dialed strings tested as part of the compliance test. All dialed strings are mapped to **Route Pattern 20** which contains the SIP trunk to the service provider (as defined next).

```
change ars analysis 0                                           Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 1

          Dialed           Total     Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
            0             1    15    20        pubu          n
```

Figure 21: ARS Analysis Form

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used in route pattern **20** for the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **20** was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format**: Set this field to **unk-unk** since private Numbering Format should be used for this route (see **Section 0**).

```
change route-pattern 20                                          Page   1 of   3
                    Pattern Number: 5   Pattern Name: SP
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 20    0                                                            n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                unk-unk   none
 2: y y y y y n  n            rest                                          none
 3: y y y y y n  n            rest                                          none
 4: y y y y y n  n            rest                                          none
```

Figure 22: Route–Pattern Form

5.11. Incoming Call Handling Treatment

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via an Adaptation. Therefore, the Communication Manager incoming call handling treatment table may not be necessary. If the DID number sent by the Service Provider is unchanged by Session Manager, then this DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group **20**. As an example, use the **change inc-call-handling-trmt trunk-group 20** to convert incoming DID numbers 44207190XXXX to 4 digit extension XXXX by deleting **8** of the incoming digits. The incoming DID number **442071900054** is converted to **8000** for voicemail testing purpose.

```
change inc-call-handling-trmt trunk-group 21                  Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/           Number     Number          Del Insert
 Feature            Len        Digits
 public-ntwrk       12         442071900054    12   8000
 public-ntwrk       12         44207190        8
```

Figure 23: Inc-Call-Handling-Trmt Form

5.12. Avaya Aura® Communication Manager Stations

In the sample configuration, four digit station extensions were used with the format 005X. Use the **add station 0050** command to add an Avaya H.323 IP Deskphone.

- Enter **Type**: **9640**, **Name**: **442071900050**, **Security Code**: **1234**, **Coverage Path 1**: **1**, **IP SoftPhone**: **y** (if using this extension as a Softphone such as Avaya one-X® Communicator).
- Leave other values as default.

```
add station 0050                                            Page   1 of   5
                                     STATION

Extension: 0050                           Lock Messages? n                 BCC: 0
     Type: 9640                             Security Code: 1234             TN: 1
     Port: S000011                        Coverage Path 1: 1               COR: 1
     Name: 442071900050                   Coverage Path 2:                 COS: 1
                                       Hunt-to Station:                  Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 0050
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: English                  Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                             IP SoftPhone? y

                                                  IP Video softphone? n
                                  Short/Prefixed Registration Allowed: default


                                              Customizable Labels? y
```

Figure 24: Station Form

5.13. Save Avaya Aura® Communication Manager Configuration Changes

Use the **save translation** command to save the configuration.

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- SIP Domain.
- Logical/physical Location that can be occupied by SIP Entities.
- SIP Entities corresponding to Communication Manager, Avaya SBCE and Session Manager.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which define route destinations and control call routing between the SIP Entities.
- Dial Patterns, which specify dialed digits and govern which Routing Policy is used to service a call.

It may not be necessary to create all the items above when configuring a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP Domains, Locations, SIP Entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL as **https://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. At the **System Manager Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button (not shown). The initial screen shown below is then displayed.

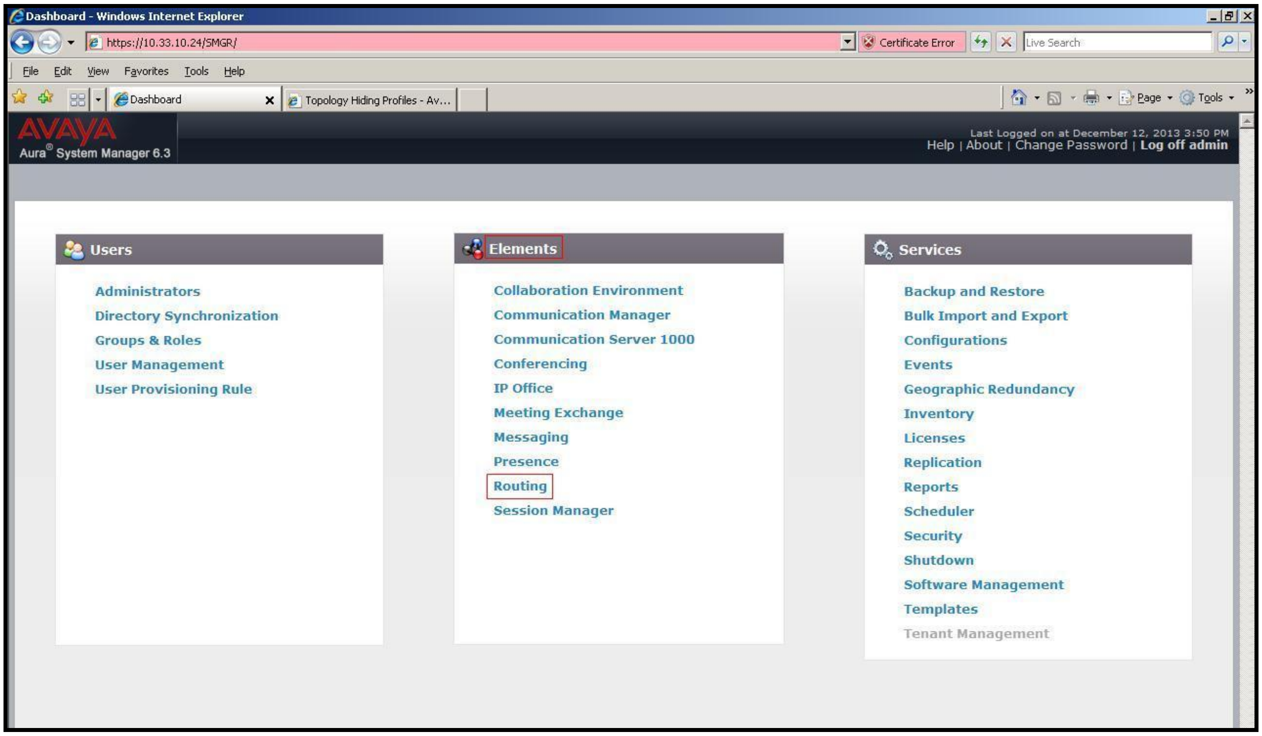
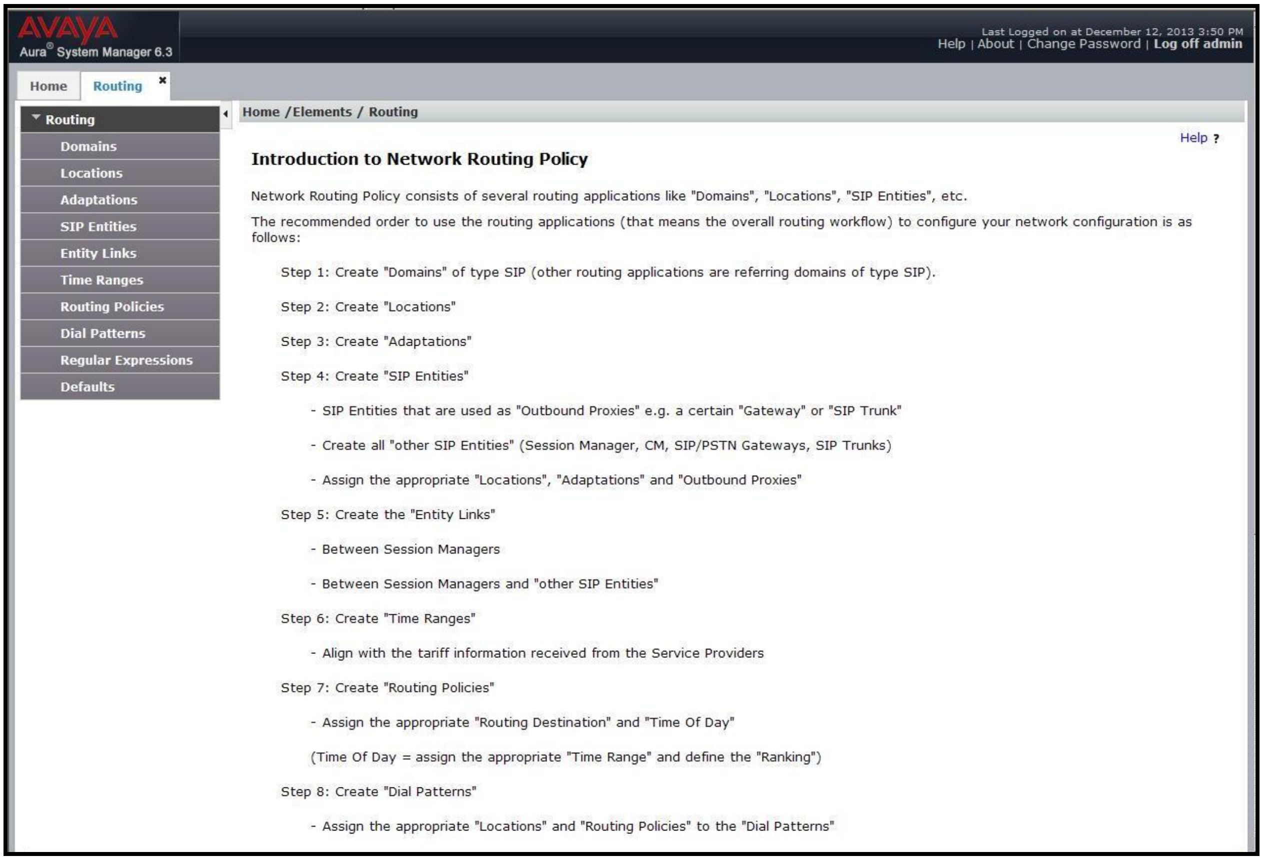


Figure 25 – System Manager Home Screen

Most of the configuration items are performed in the Routing Element. Click on **Routing** in the **Elements** column to bring up the **Introduction to Network Routing Policy** screen.

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.



Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

- Assign the appropriate "Routing Destination" and "Time Of Day"

(Time Of Day = assign the appropriate "Time Range" and define the "Ranking")

Step 8: Create "Dial Patterns"

- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"

Figure 26 – Network Routing Policy

6.2. Specify SIP Domain

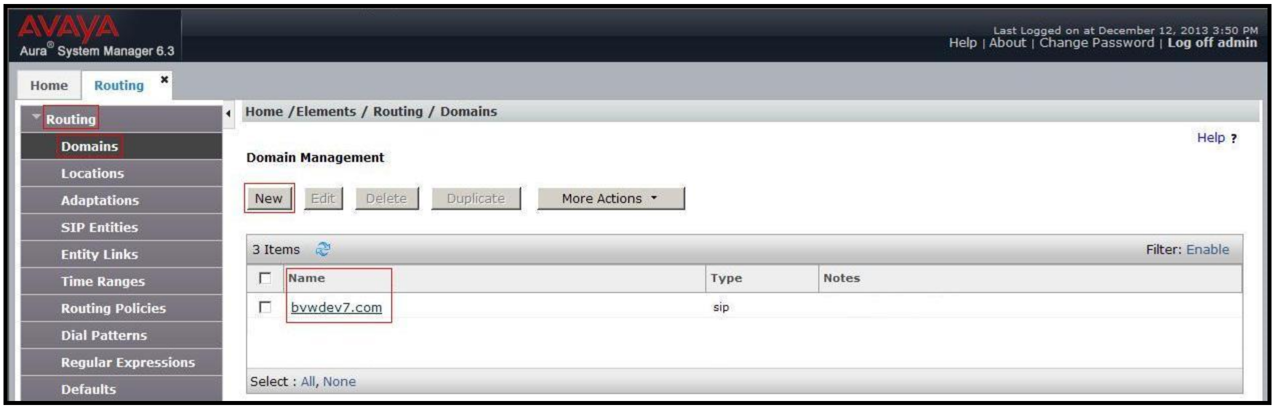
Create a SIP Domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain **bvwdev7.com**.

Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane. In the new right pane that appears (not shown), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit** (not shown) to save.

The screen below shows the existing entry for the enterprise domain.



☐	Name	Type	Notes
☐	bvwdev7.com	sip	

Figure 27 – Domain Management

6.3. Add Location

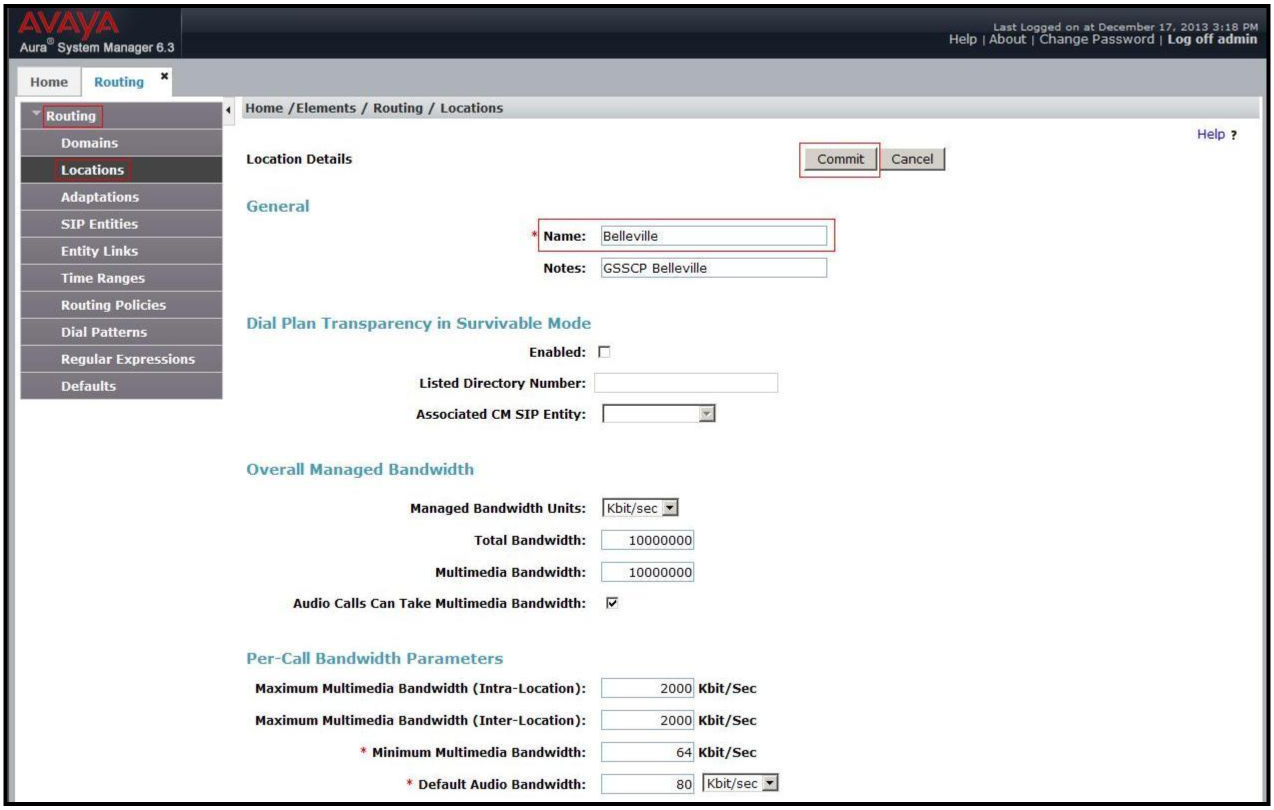
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **Belleville**, which includes all equipment in the enterprise including Communication Manager, Session Manager and Avaya SBCE.

To add a Location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name for the Location.
- **Notes:** Add a brief description (optional).

Click **Commit** to save.



Location Details

General

* Name: Belleville

Notes: GSSCP Belleville

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth: 10000000

Multimedia Bandwidth: 10000000

Audio Calls Can Take Multimedia Bandwidth: ☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec

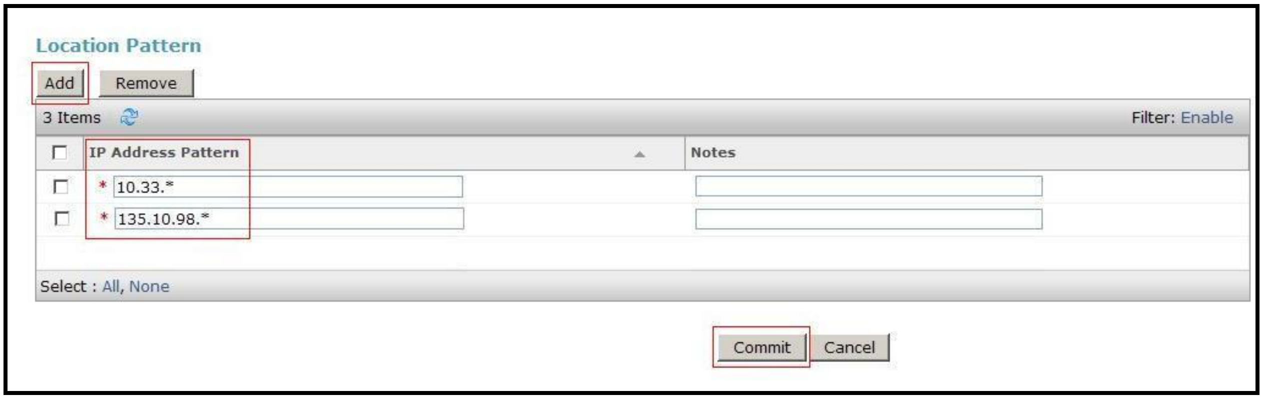
* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Figure 28 – Location Configuration

In the **Location Pattern** section, click **Add** to enter IP Address patterns. The following patterns were used in testing:

- **IP Address Pattern:** 10.33.*, 10.10.98.*



☐	IP Address Pattern	Notes
☐	* 10.33.*	
☐	* 135.10.98.*	

Figure 29 – IP Ranges Configuration

Click **Commit** to save.

Note that call bandwidth management parameters should be set per customer requirement.

6.4. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and Avaya SBCE.

Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

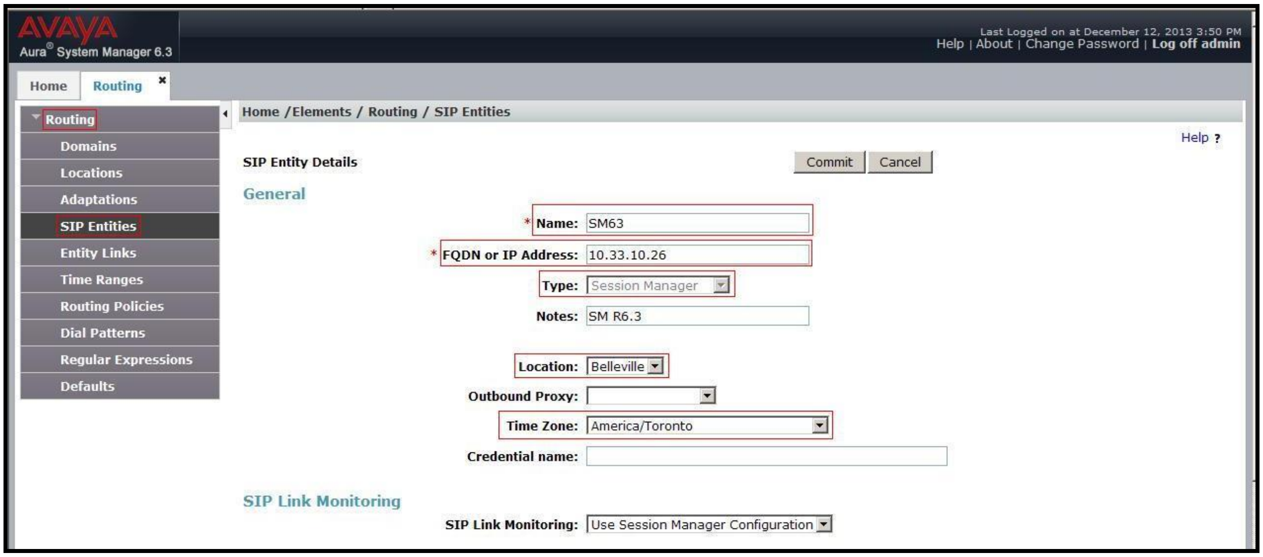
Name:	Enter a descriptive name.
FQDN or IP Address:	Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
Type:	Select **Session Manager** for Session Manager, **CM** for Communication Manager and **Other** for Avaya SBCE.
Adaptation:	This field is only present if **Type** is not set to **Session Manager**. Adaptation module was not used in this configuration.
Location:	Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location **Belleville**.
Time Zone:	Select the time zone for the Location above.

In this configuration, there are three SIP Entities.

- Session Manager SIP Entity.
- Communication Manager SIP Entity.
- Avaya Session Border Controller for Enterprise SIP Entity.

6.4.1. Configure Session Manager SIP Entity

The following screen shows the addition of the Session Manager SIP Entity named **SM63**. The IP address of Session Manager's signaling interface is entered for **FQDN or IP Address 10.33.10.26**. Select **Location** as **Belleville** and select **Time Zone** as **America/Toronto**.



* Name: SM63

* FQDN or IP Address: 10.33.10.26

Type: Session Manager

Notes: SM R6.3

Location: Belleville

Outbound Proxy:

Time Zone: America/Toronto

Credential name:

SIP Link Monitoring: Use Session Manager Configuration

Figure 30 – Session Manager SIP Entity

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

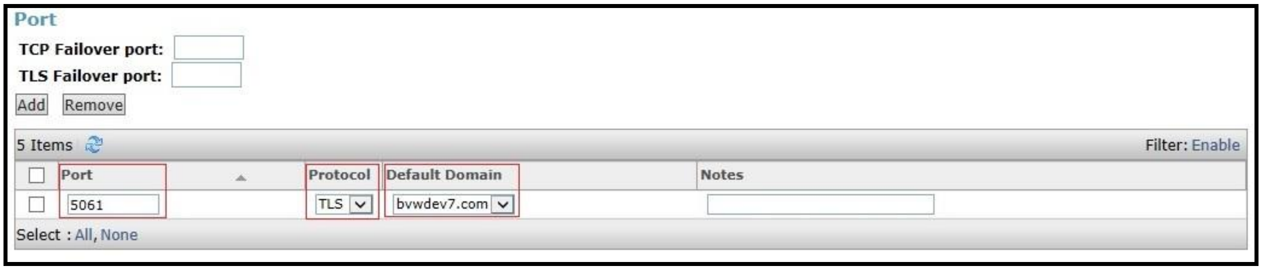
In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port:**	Port number on which Session Manager listens for SIP requests.
- **Protocol:**	Transport protocol to be used with this port.
- **Default Domain:**	The default domain associated with this port. For the compliance test, this was the enterprise SIP Domain.

Defaults can be used for the remaining fields. Click **Commit** (not shown) to save.

The compliance test used port **5061** with **TLS** for connecting to Communication Manager, Avaya SIP telephones and SIP soft clients, and Avaya SBCE.

Other entries defined for other projects as shown in the screen were not used.



Port

TCP Failover port:

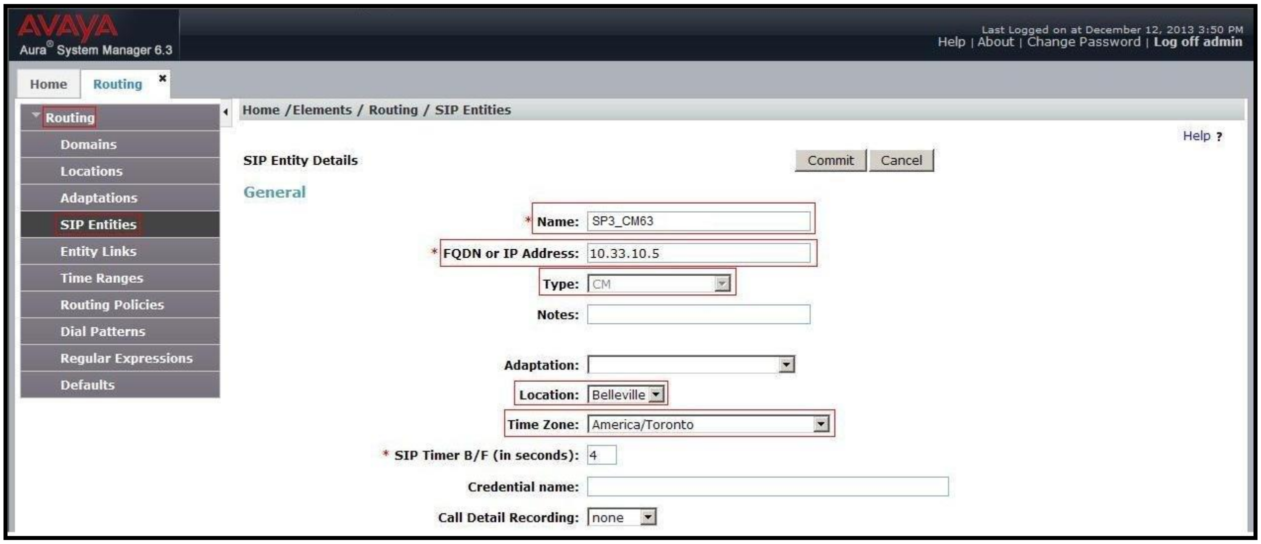
TLS Failover port:

☐	Port	Protocol	Default Domain	Notes
☐	5061	TLS	bvwdev7.com	

Figure 31 – Session Manager SIP Entity Port

6.4.2. Configure Communication Manager SIP Entity

The following screen shows the addition of the Communication Manager SIP Entity named **SP3_CM63**. In order for Session Manager to send SIP service provider traffic on a separate Entity Link to Communication Manager, it is necessary to create a separate SIP Entity for Communication Manager in addition to the one created during Session Manager installation. The original SIP entity is used with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP address of Communication Manager **10.33.10.5**. Note that **CM** was selected for **Type**. The **Location** field is set to **Belleville** which is the Location that includes the subnet where Communication Manager resides. Select **Time Zone** as **America/Toronto**.



SIP Entity Details

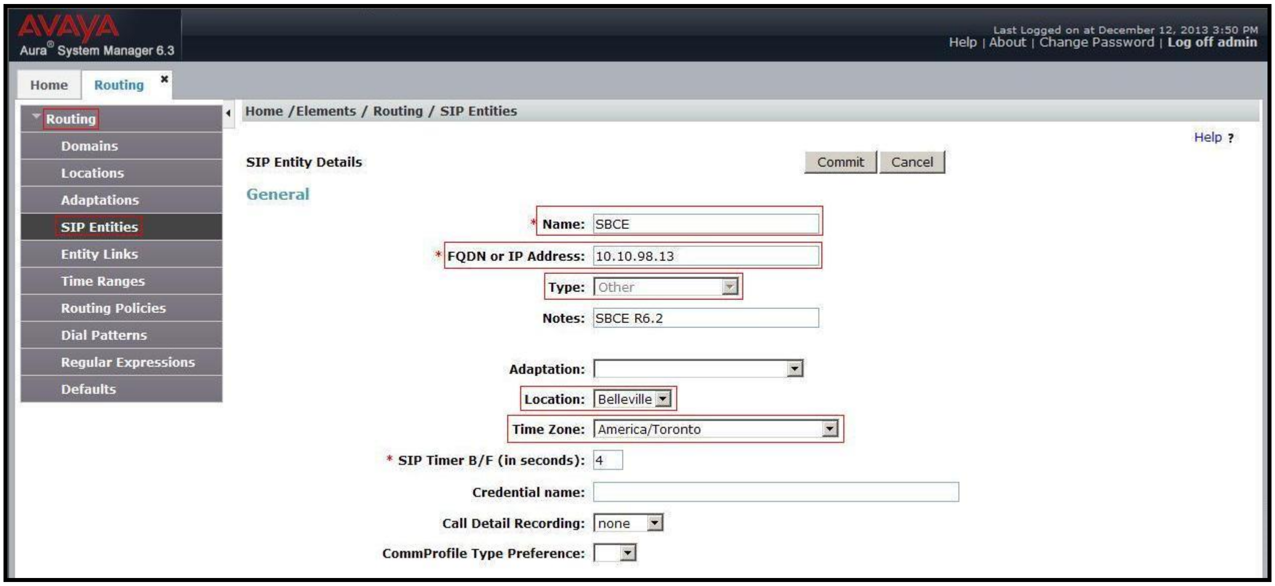
General

* Name: SP3_CM63
* FQDN or IP Address: 10.33.10.5
Type: CM
Notes:
Adaptation:
Location: Belleville
Time Zone: America/Toronto
* SIP Timer B/F (in seconds): 4
Credential name:
Call Detail Recording: none

Figure 32 – Communication Manager SIP Entity

6.4.3. Configure Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the addition of the Avaya SBCE SIP entity named **SBCE**. The **FQDN** or **IP Address** field is set to the IP address of the SBC's private network interface **10.10.98.13**. Note that **Other** was selected for **Type**. The **Location** field is set to **Belleville** which includes the subnet where the Avaya SBCE resides. Select **Time Zone** as **America/Toronto**.



SIP Entity Details

General

* Name: SBCE

* FQDN or IP Address: 10.10.98.13

Type: Other

Notes: SBCE R6.2

Adaptation:

Location: Belleville

Time Zone: America/Toronto

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Figure 33 – Avaya SBCE SIP Entity

6.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by service provider traffic and one to the Avaya SBCE.

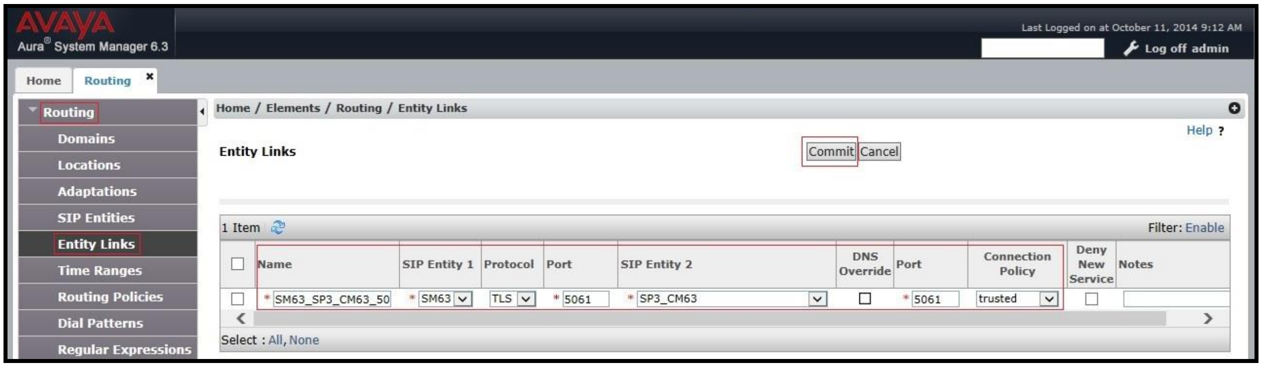
To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager being used.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. (Ex: For the Communication Manager Entity Link, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 0**).
- **SIP Entity 2:** Select the name of the other system as defined in **Section 6.4**.

- **Port:** Port number on which the other system receives SIP requests from the Session Manager. (Ex: For the Communication Manager Entity Link, this must match the Near-end Listen Port defined on the Communication Manager signaling group in **Section 0**).
- **Trusted:** Check this box. Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.4** will be denied.

Click **Commit** to save.

The following screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 0**.

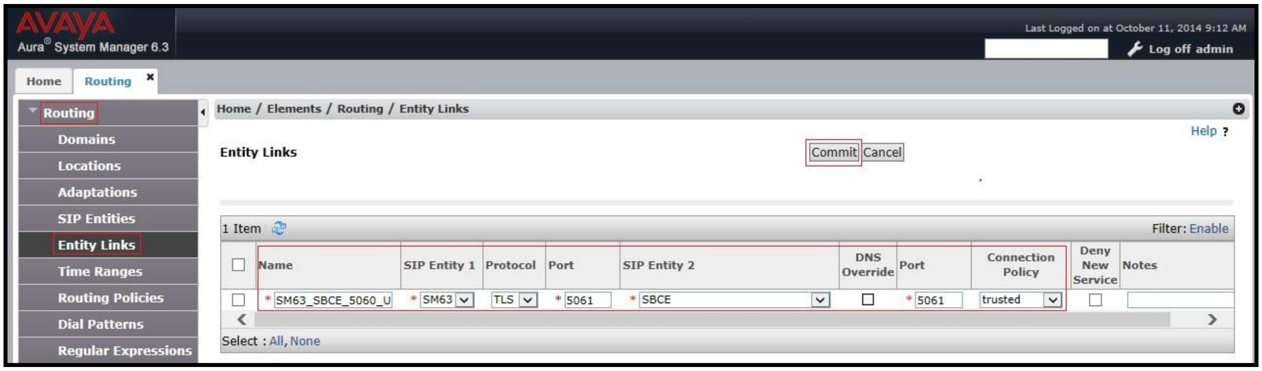


Entity Links

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
☐	* SM63_SP3_CM63_50	* SM63	TLS	* 5061	* SP3_CM63	☐	* 5061	trusted	☐	

Figure 34 – Communication Manager Entity Link

The following screen illustrates the Entity Links to Avaya SBCE. The protocol and ports defined here must match the values used on the Avaya SBCE mentioned in **Section 7.3.4** and **7.3.7**.



Entity Links

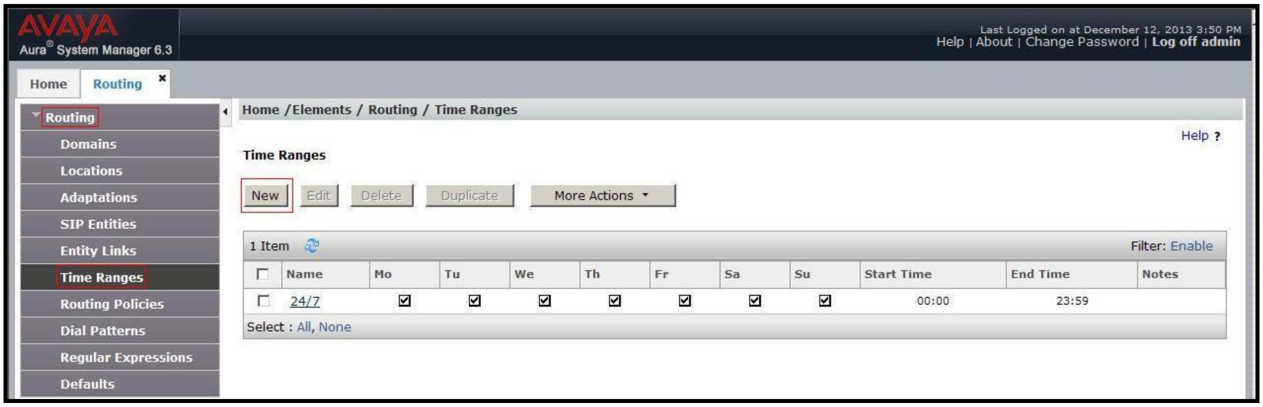
1 Item

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
☐	* SM63_SBCE_5060_U	* SM63	TLS	* 5061	* SBCE	☐	* 5061	trusted	☐	

Figure 35 – Avaya SBCE Entity Link

6.6. Configure Time Ranges

Time Ranges is configured for time-based-routing. In order to add Time Ranges, select **Routing → Time Ranges** and then click **New** button. The Routing Policies shown subsequently will use the 24/7 range since time-based routing was not the focus of these Application Notes.



Time Ranges

1 Item

☐	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
☐	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	

Figure 36 – Time Ranges

6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two Routing Policies must be added: one for Communication Manager and one for Avaya SBCE.

To add a Routing Policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

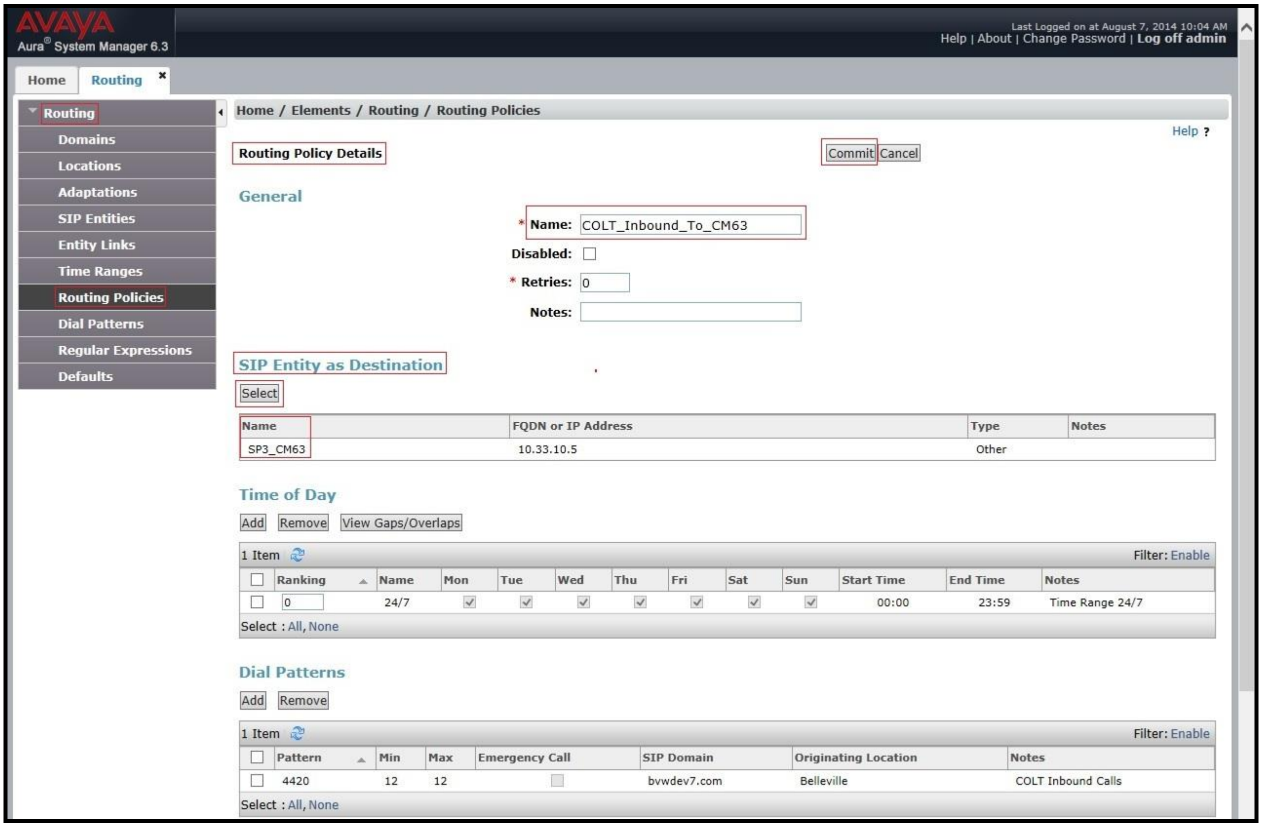
In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP Entity to which this Routing Policy applies and click **Select**. The selected SIP Entity displays on the Routing Policy Details page as shown below. Use default values for remaining fields.

Click **Commit** to save.

The following screen shows the **Routing Policy Details** for the policy named **COLT_Inbound_To_CM63** associated with incoming PSTN calls from COLT to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **SP3_CM63**.



Routing Policy Details

General

Name: COLT_Inbound_To_CM63
Disabled: ☐
Retries: 0
Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
SP3_CM63	10.33.10.5	Other	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

☐	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add Remove

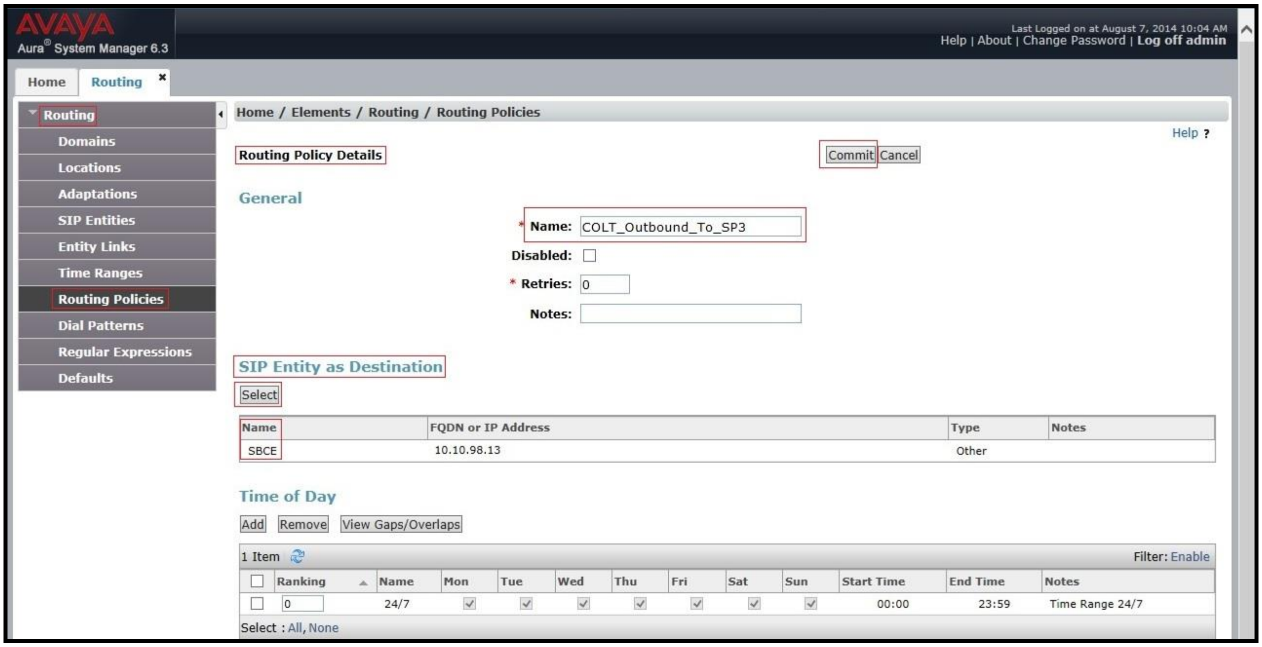
1 Item Filter: Enable

☐	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	4420	12	12	☐	bvwdev7.com	Belleville	COLT Inbound Calls

Select : All, None

Figure 37 – Routing to Communication Manager

The following screen shows the **Routing Policy Details** for the policy named **COLT_Outbound_To_SP3** associated with outgoing calls from Communication Manager to the PSTN via COLT through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **SBCE**.



Routing Policy Details

General

Name: COLT_Outbound_To_SP3

Disabled: ☐

Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
SBCE	10.10.98.13	Other	

Time of Day

1 Item

☐	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Figure 38 – Routing to COLT

6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were configured to route calls from Communication Manager to COLT through the Avaya SBCE and vice versa. Dial Patterns define which Route Policy will be selected as route destination for a particular call based on the dialed digits, destination Domain and originating Location.

To add a Dial Pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

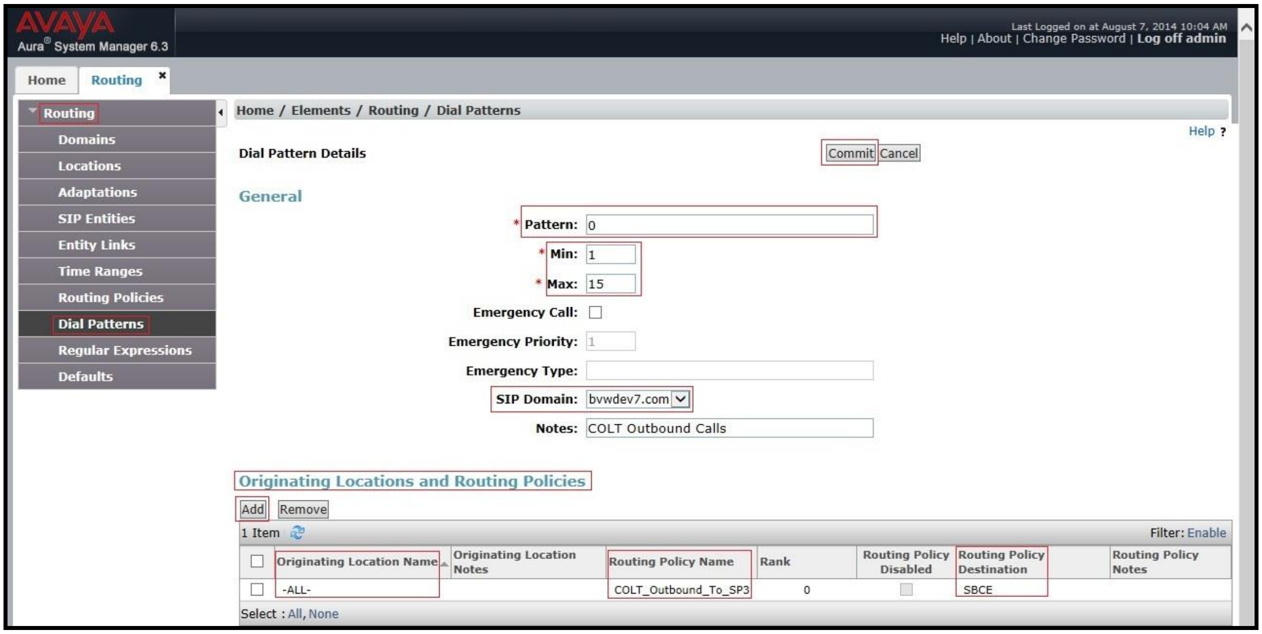
- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating Location for use in the match criteria. Lastly, select the Routing Policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the Dial Patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other Dial Patterns were similarly defined.

The first example shows that outbound maximum 15-digit dialed numbers that begin with **0** and have a destination SIP Domain of **bvwdev7.com** uses Routing Policy Name **COLT_Outbound_To_SP3** as defined in **Section 6.7**.



Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

* Pattern: 0

* Min: 1

* Max: 15

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwdev7.com

Notes: COLT Outbound Calls

Originating Locations and Routing Policies

1 Item — Filter: Enable

☐	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	-ALL-		COLT_Outbound_To_SP3	0	☐	SBCE	

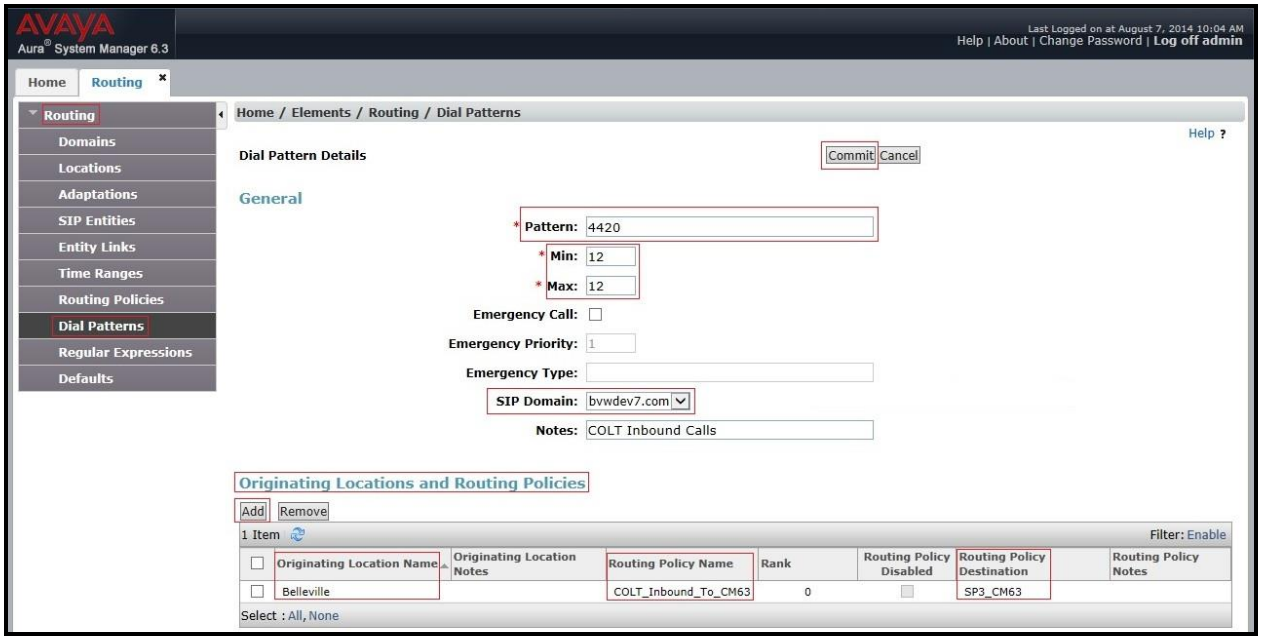
Select : All, None

Figure 39 – Dial Pattern_0

Note that the above Dial Pattern did not restrict outbound calls to specific US area codes. In real deployments, appropriate restriction can be exercised per customer business policies.

Also note that **-ALL-** was selected for **Originating Location Name**. This selection was chosen to accommodate certain off-net call forward scenarios where the inbound call was re-directed outbound back to the PSTN.

The second example shows that inbound 12-digit numbers that start with **4420** uses Routing Policy Name **COLT_Inbound_To_CM63** as defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by COLT.



Dial Pattern Details

General

Pattern: 4420
Min: 12
Max: 12
Emergency Call: ☐
Emergency Priority: 1
Emergency Type:
SIP Domain: bvwdev7.com
Notes: COLT Inbound Calls

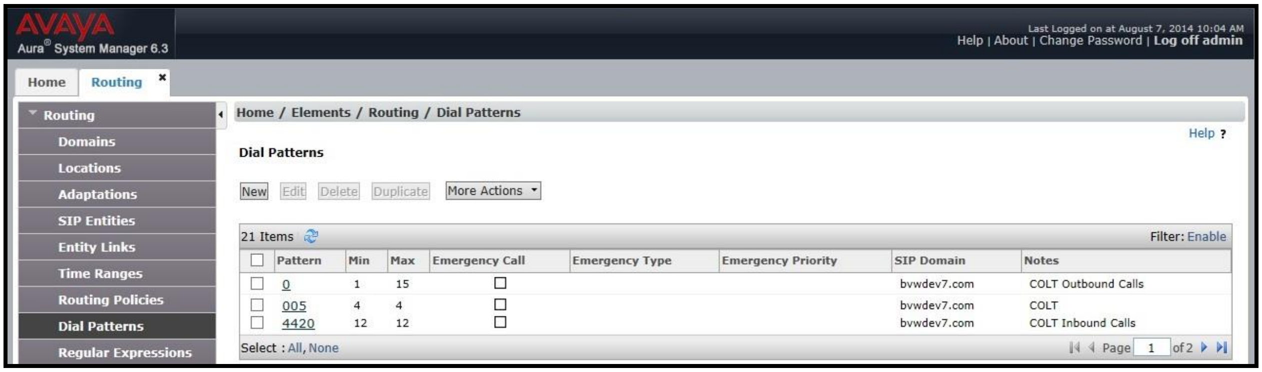
Originating Locations and Routing Policies

1 Item

☐	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Belleville		COLT_Inbound_To_CM63	0	☐	SP3_CM63	

Figure 40 – Dial Pattern_4420

The following screen illustrates a list of dial patterns used for inbound and outbound calls between the enterprise and the PSTN.



Dial Patterns

21 Items

☐	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
☐	0	1	15	☐			bvwdev7.com	COLT Outbound Calls
☐	005	4	4	☐			bvwdev7.com	COLT
☐	4420	12	12	☐			bvwdev7.com	COLT Inbound Calls

Figure 41 – Dial Pattern List

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE necessary for interoperability with the Session Manager and the COLT system.

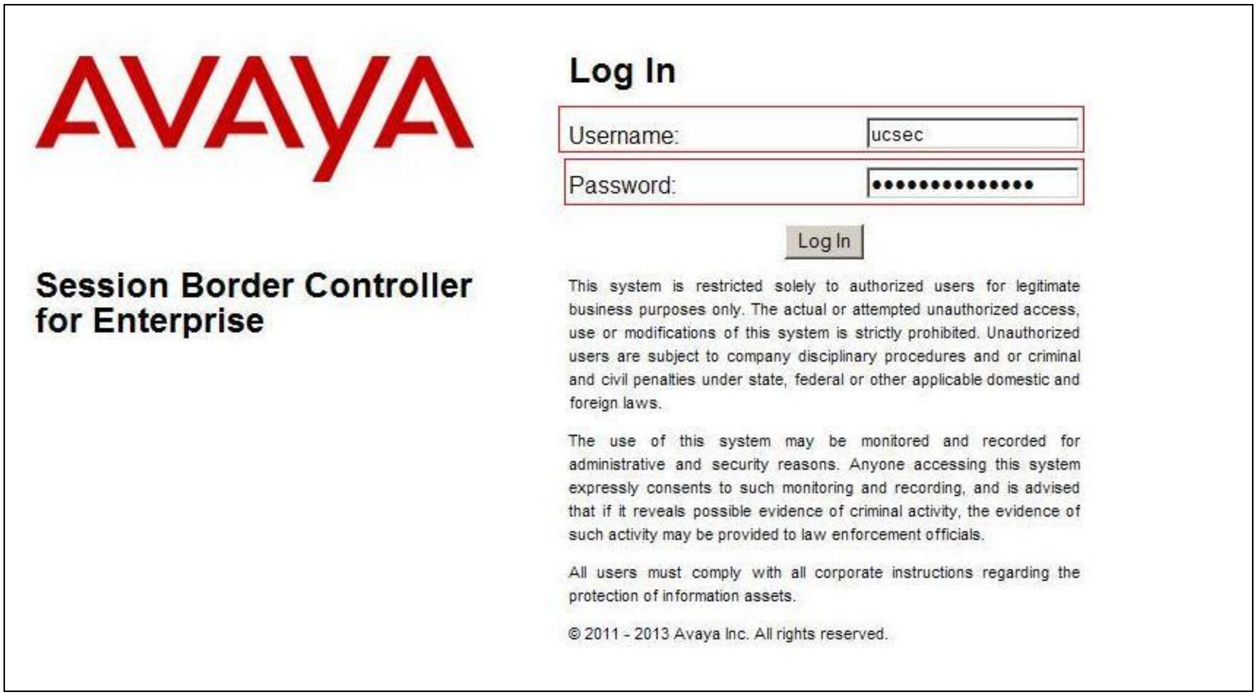
In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the COLT system resides on the Public side of the network.

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, see **Section 11** of these Application Notes.

7.1. Log in Avaya Session Border Controller for Enterprise

Access the web interface by typing "**https://x.x.x.x/sbc/**" (where x.x.x.x is the management IP of the Avaya SBCE).

Enter the **Username** and **Password**.



Username: ucsec

Password: ••••••••••••••

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

Figure 42 - Avaya SBCE Login

7.2. TLS Management

7.2.1. Installing TLS Certificate

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. UC-Sec security products utilize TLS primarily to facilitate secure communications with remote users.

To manage TLS parameters:

- Avaya provided the Avaya root certificate to COLT to validate Avaya certificate (Note: COLT requested for the root certificate in *.der format. But the original Avaya root certificate was in *.crt format, therefore there is a need to use any tools such as openssl *commands openssl x509 -in <in cert file> -inform pem -out <der cert file name> -outform der* to convert from *.crt format to *.der format).
- On the other hand, COLT provided COLT root certificate to validate COLT certificate. (Note: COLT provided the certificate in *.cer format. It should be converted to *.crt format before installing it in Avaya SBCE).
- On Avaya SBCE, install COLT root certificate as Certificate Authority (CA) certificate.
- Once these procedures are completed, create a client profile and a server profile.

It is assumed generating of the Certificates have been previously completed and is not discussed here.

The following paragraph is an overview of the mutual certificate authentication that is being used for this application:

For the Avaya site

- Avaya Session Manager has certs “B” and “CAa” uploaded.
- Avaya SBCE has certs “A” and “CAb” uploaded.
- During the TLS authentication process/handshake, certificate “A” is sent from the Avaya SBCE to Session Manager. CA certificate “CAa” is used by Session Manager to validate certificate “A”.
- Session Manager sends certificate “B” to the Avaya SBCE. CA certificate “CAb” is used by the Avaya SBCE to validate certificate “B”.

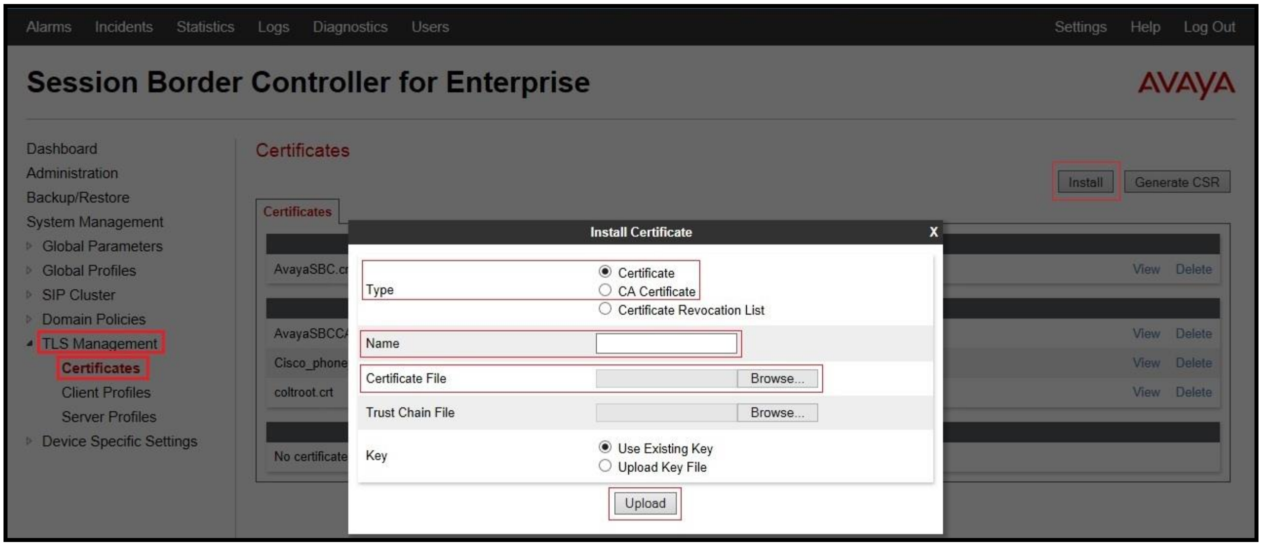
For the COLT site

- COLT has certs “D” and “CAa” uploaded.
- Avaya SBCE has certs “A” and “CAd” uploaded.
- During the TLS authentication process/handshake, certificate “A” is sent from the Avaya SBCE to COLT. CA certificate “CAa” is used by COLT to validate certificate “A”.
- COLT sends certificate “D” to the Avaya SBC. CA certificate “CAd” is used by the Avaya SBC to validate certificate “D”.

The following procedures show how to install the certificates, and create client and server profiles.

From the left hand site menu, select **TLS Management → Certificates** and click on **Install** button located in the upper-right hand.

- Select **Type**: **Certificate** for installing Avaya Identity certificate; **CA Certificate** for installing COLT and Avaya Session Manager root certificates.
- Enter **Name**: **AvayaSBC** for installing Avaya Identity certificate, **coltroot** for installing COLT root certificate, and **AvayaSBCCA** for installing Avaya Session Manager root certificate.
- Click **Browse** button to navigate to the Certificate File. Choose the certificates accordingly.
- Click **Upload**.



Type: ● Certificate ○ CA Certificate ○ Certificate Revocation List

Name:

Certificate File:

Trust Chain File:

Key: ● Use Existing Key ○ Upload Key File

Figure 43 – Certificate Installation

The following screen shows the installed certificates for both Avaya and COLT.

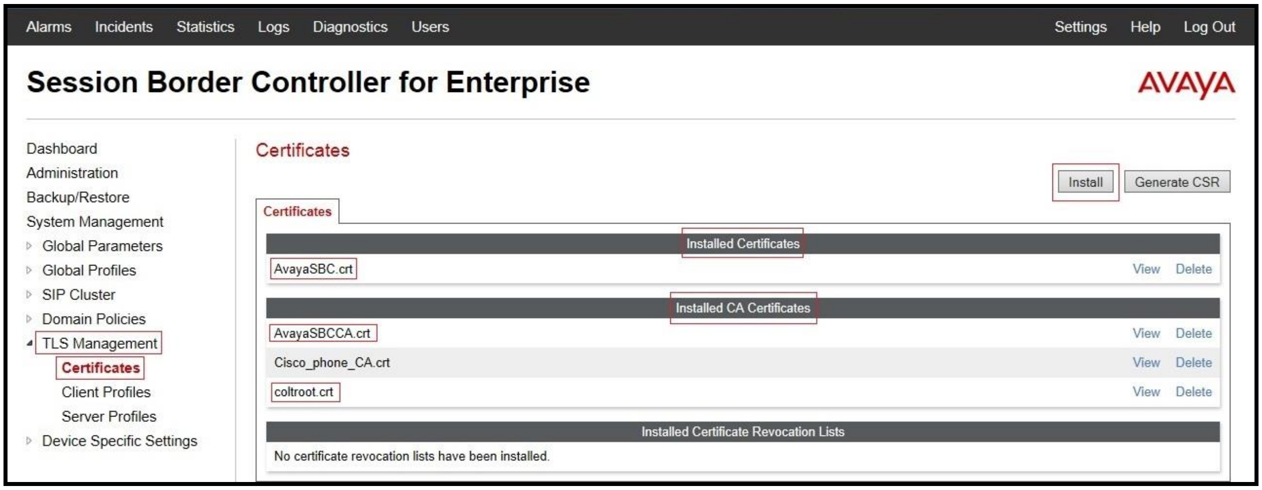
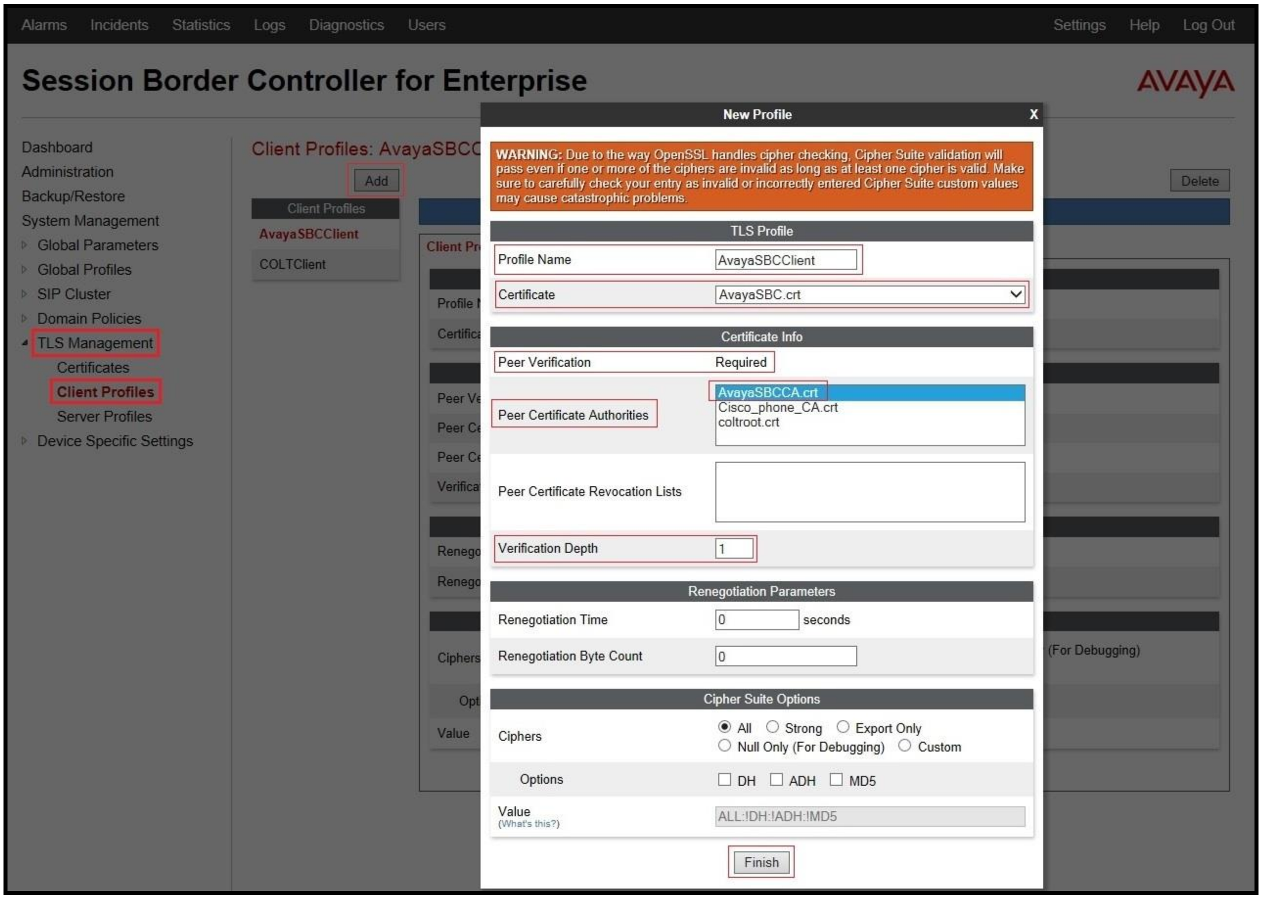


Figure 44 – The installed certificates for both Avaya and COLT

7.2.2. TLS Client Profile for Avaya site

From the menu on the left-hand side, select **TLS Management → Client Profiles**

- Select **Add** the **Client Profiles**.
- Enter **Profile Name**: **AvayaSBCClient**.
- Select **Certificate**: **AvayaSBC.crt**.
- The **Peer Verification** is always **Required**.
- Select **Peer Certificate Authorities: AvayaSBCCA.crt** to peer with Session Manager.
- Enter **Verification Depth**: **1**.
- Click **Finish**.



WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

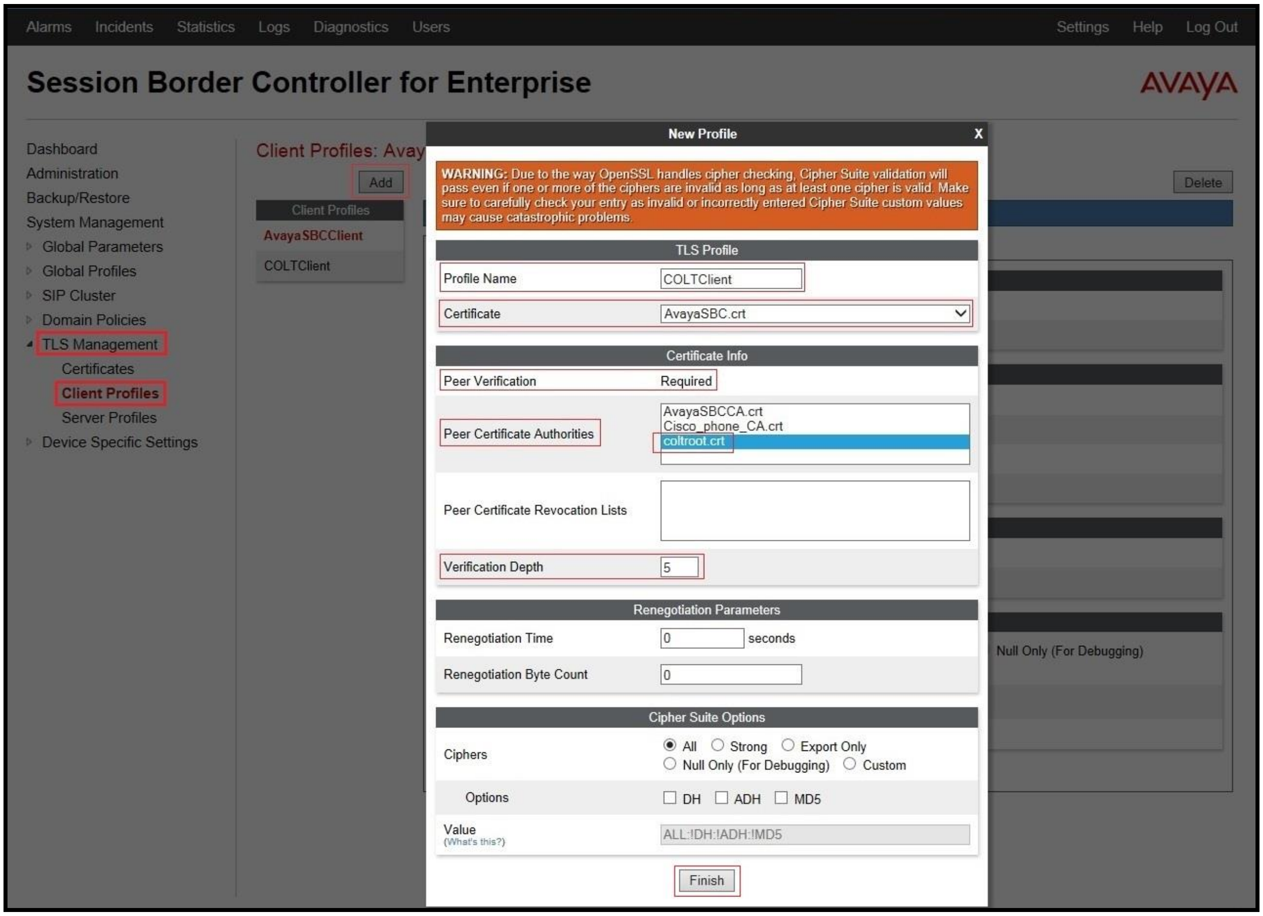
TLS Profile	
Profile Name	AvayaSBCClient
Certificate	AvayaSBC.crt
Certificate Info	
Peer Verification	Required
Peer Certificate Authorities	AvayaSBCCA.crt Cisco_phone_CA.crt coltroot.crt
Peer Certificate Revocation Lists	
Verification Depth	1
Renegotiation Parameters	
Renegotiation Time	0 seconds
Renegotiation Byte Count	0
Cipher Suite Options	
Ciphers	● All ○ Strong ○ Export Only ○ Null Only (For Debugging) ○ Custom
Options	☐ DH ☐ ADH ☐ MD5
Value (What's this?)	ALL:!DH:!ADH:!MD5

Figure 45 – TLS Client Profile - Avaya site

7.2.3. TLS Client Profile for COLT site

From the menu on the left-hand side, select **TLS Management → Client Profiles**

- Select **Add** the **Client Profiles**.
- Enter **Profile Name**: **COLTClient**.
- Select **Certificate**: **AvayaSBC.crt**.
- The **Peer Verification** is always **Required**.
- Select **Peer Certificate Authorities: coltroot.crt** to peer with COLT.
- Enter **Verification Depth**: **5**.
- Click **Finish**.



WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

TLS Profile	
Profile Name	COLTClient
Certificate	AvayaSBC.crt

Certificate Info	
Peer Verification	Required
Peer Certificate Authorities	AvayaSBCCA.crt Cisco_phone_CA.crt coltroot.crt
Peer Certificate Revocation Lists	
Verification Depth	5

Renegotiation Parameters	
Renegotiation Time	0 seconds
Renegotiation Byte Count	0

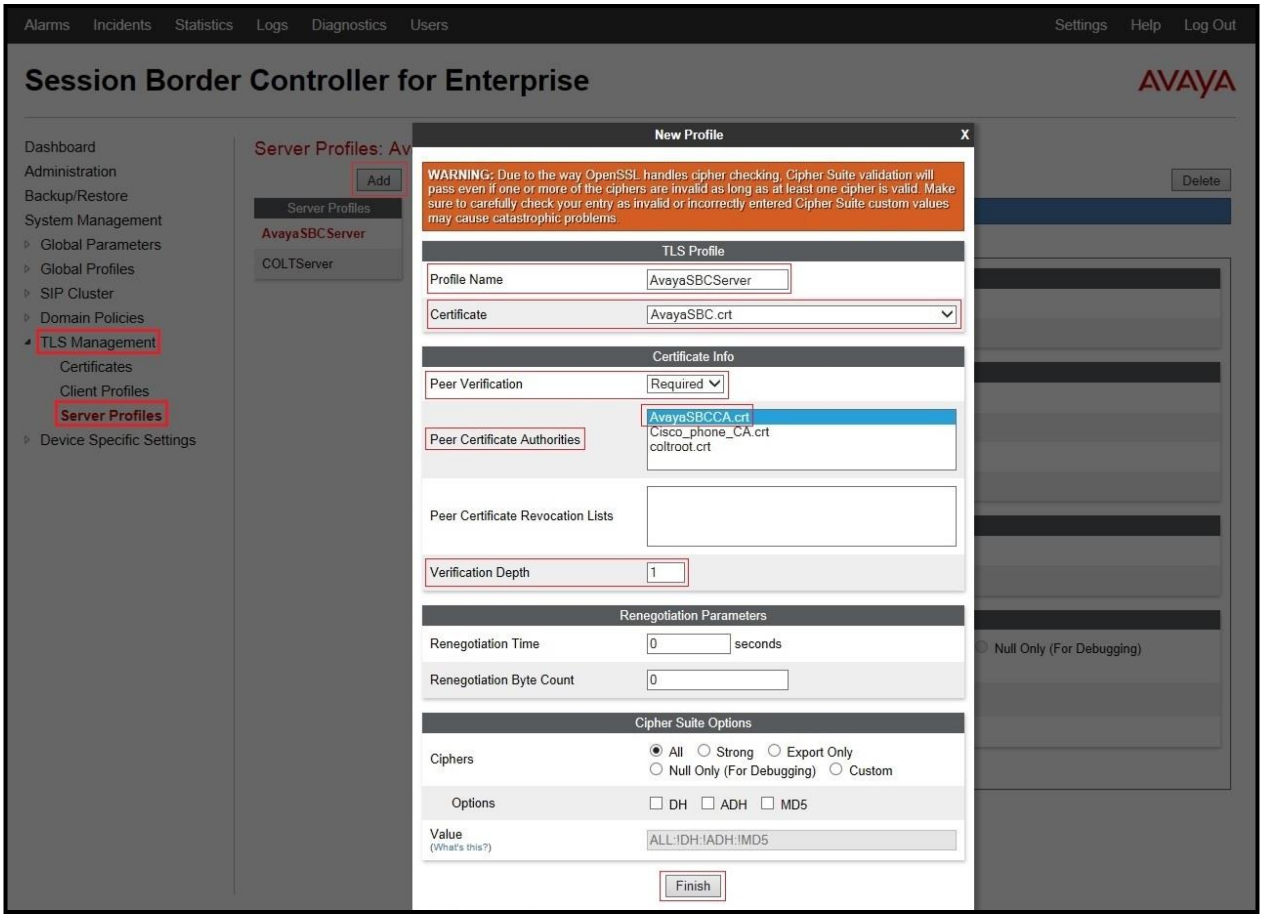
Cipher Suite Options	
Ciphers	● All ○ Strong ○ Export Only ○ Null Only (For Debugging) ○ Custom
Options	☐ DH ☐ ADH ☐ MD5
Value (What's this?)	ALL:!DH:!ADH:!MD5

Figure 46 – TLS Client Profile - COLT site

7.2.4. TLS Server Profile for Avaya site

From the menu on the left-hand side, select **TLS Management → Server Profiles**

- Select **Add** the **Server Profiles**.
- Enter **Profile Name**: **AvayaSBCServer**.
- Select **Certificate**: **AvayaSBC.crt**.
- Select **Peer Verification**: **Required**.
- Select **Peer Certificate Authorities**: **AvayaSBCCA.crt** to peer with Session Manager.
- Enter **Verification Depth**: **1**.
- Click **Finish**.



WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

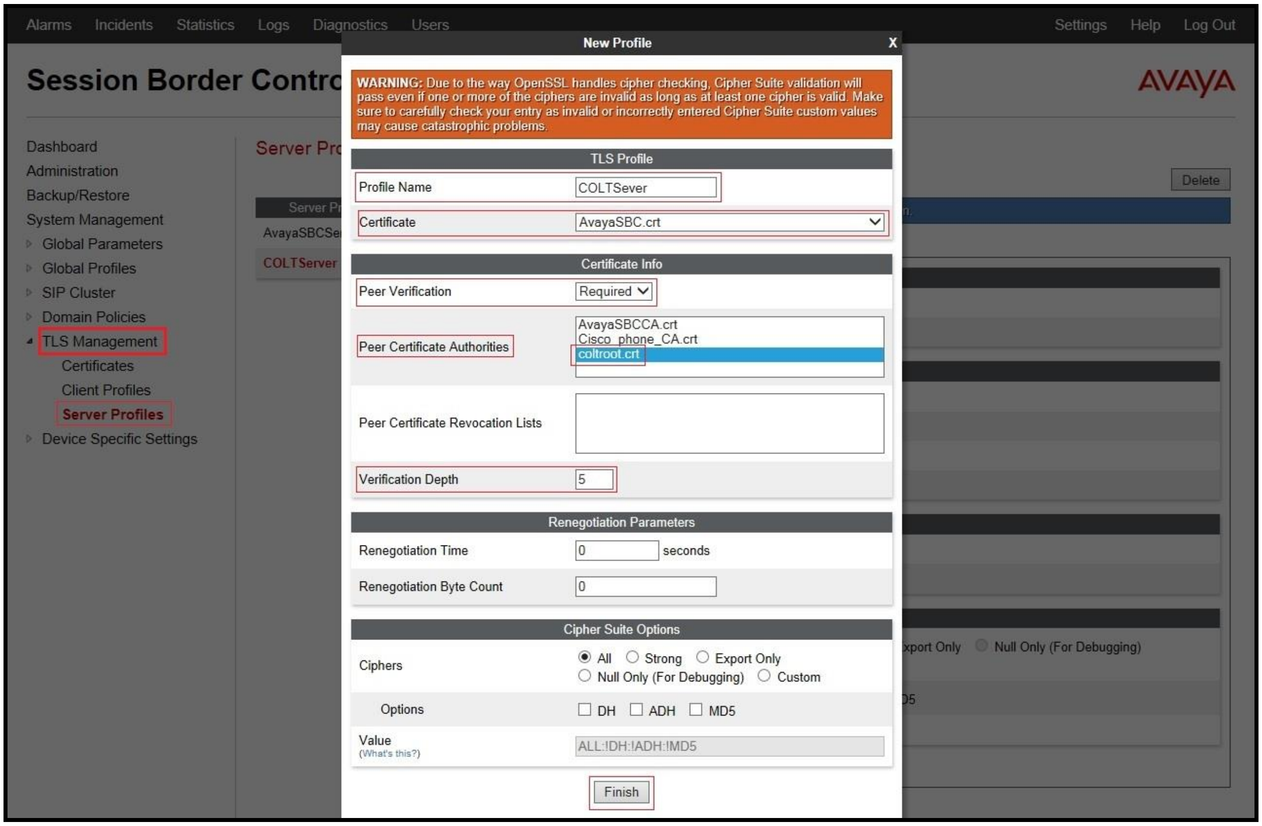
Profile Name: AvayaSBCServer
Certificate: AvayaSBC.crt
Peer Verification: Required
Peer Certificate Authorities: AvayaSBCCA.crt (selected), Cisco_phone_CA.crt, coltroot.crt
Peer Certificate Revocation Lists:
Verification Depth: 1
Renegotiation Time: 0 seconds
Renegotiation Byte Count: 0
Ciphers: ● All ○ Strong ○ Export Only ○ Null Only (For Debugging) ○ Custom
Options: ☐ DH ☐ ADH ☐ MD5
Value (What's this?): ALL:!DH:!ADH:!MD5

Figure 47 – TLS Server Profile - Avaya site

7.2.5. TLS Server Profile for COLT site

From the menu on the left-hand side, select **TLS Management → Server Profiles**

- Select **Add** the **Server Profiles**.
- Enter **Profile Name**: **COLTServer**.
- Select **Certificate**: **AvayaSBC.crt**.
- Select **Peer Verification**: **Required**.
- Select **Peer Certificate Authorities**: **coltroot.crt** to peer with COLT.
- Enter **Verification Depth**: **5**.
- Click **Finish**.



New Profile

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

TLS Profile	
Profile Name	COLTSever
Certificate	AvayaSBC.crt
Certificate Info	
Peer Verification	Required
Peer Certificate Authorities	AvayaSBCCA.crt Cisco_phone_CA.crt coltroot.crt
Peer Certificate Revocation Lists	
Verification Depth	5
Renegotiation Parameters	
Renegotiation Time	0 seconds
Renegotiation Byte Count	0
Cipher Suite Options	
Ciphers	● All ○ Strong ○ Export Only ○ Null Only (For Debugging) ○ Custom
Options	☐ DH ☐ ADH ☐ MD5
Value (What's this?)	ALL:!DH:!ADH:!MD5

Figure 48 – TLS Server Profile - COLT site

7.3. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

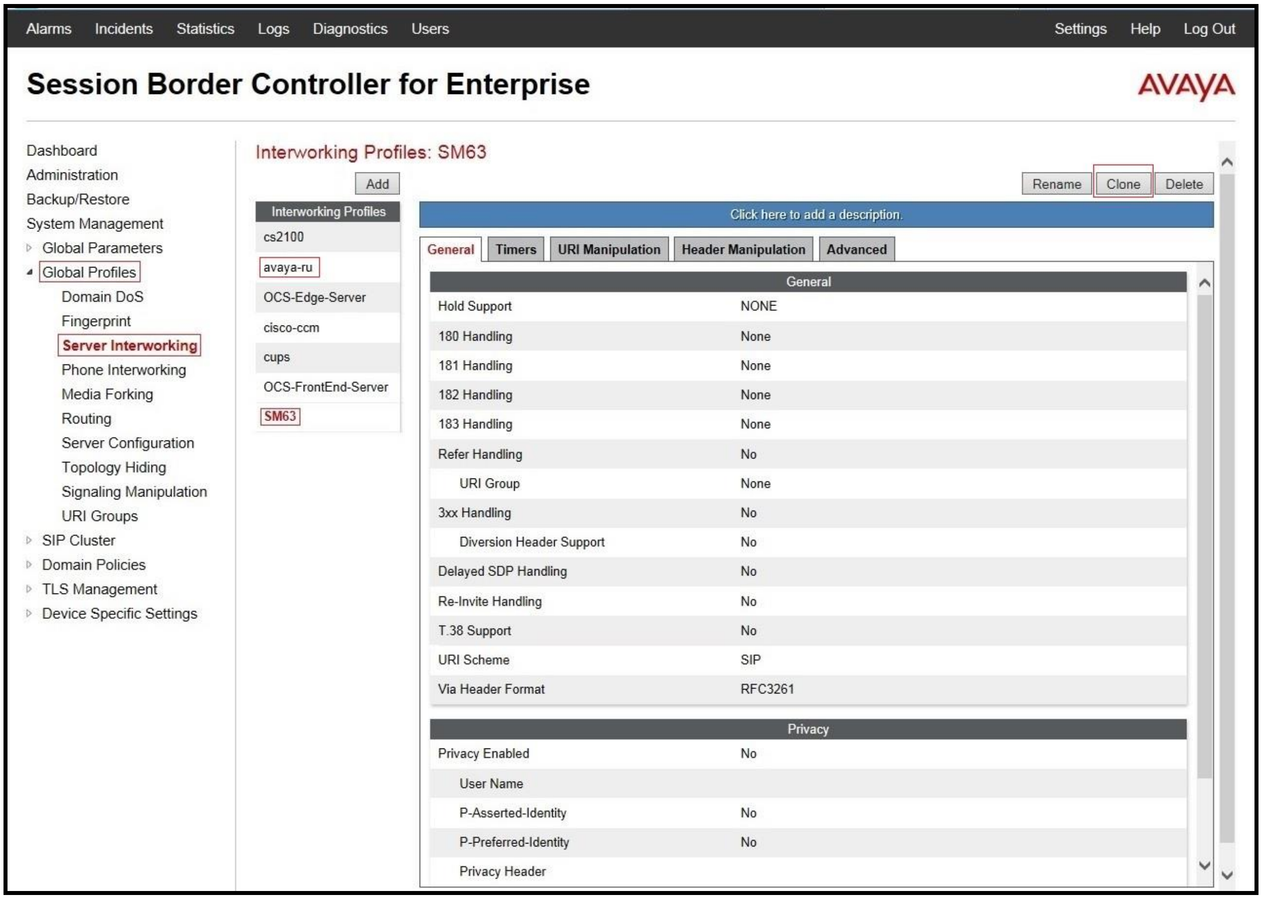
7.3.1. Configure Server Interworking Profile - Avaya site

Server Interworking profile allows administrator to configure and manage various SIP call server-specific capabilities such as call hold, 180 handling, etc.

From the menu on the left-hand side, select **Global Profiles → Server Interworking**

- Select **avaya-ru** in Interworking Profiles.
- Click **Clone**.
- Enter **Clone Name**: **SM63** and Click **Finish** (not shown).

The following screen shows that Session Manager server interworking profile (named: **SM63**) was added.



General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

Figure 49 - Server Interworking – Avaya site

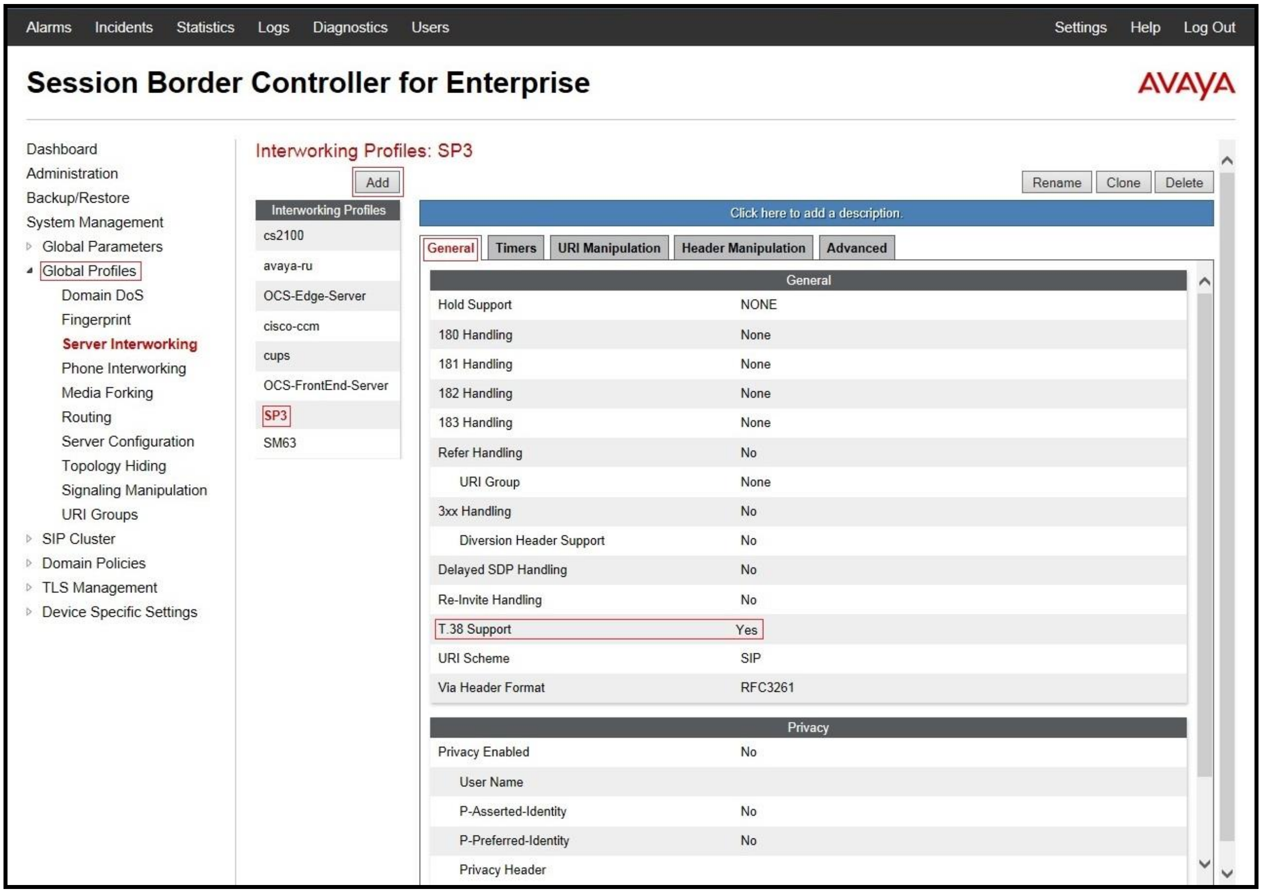
7.3.2. Configure Server Interworking Profile – COLT site

From the menu on the left-hand side, select **Global Profiles → Server Interworking → Add**

- Enter Profile name: **SP3**.
- On the **General** tab, set **T.38 Support** as **yes**. Others options can be left at default.

On the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** tabs: all options can be left at default. Click **Finish** (not shown).

The following screen shows that COLT server interworking profile (named: **SP3**) was added.



General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

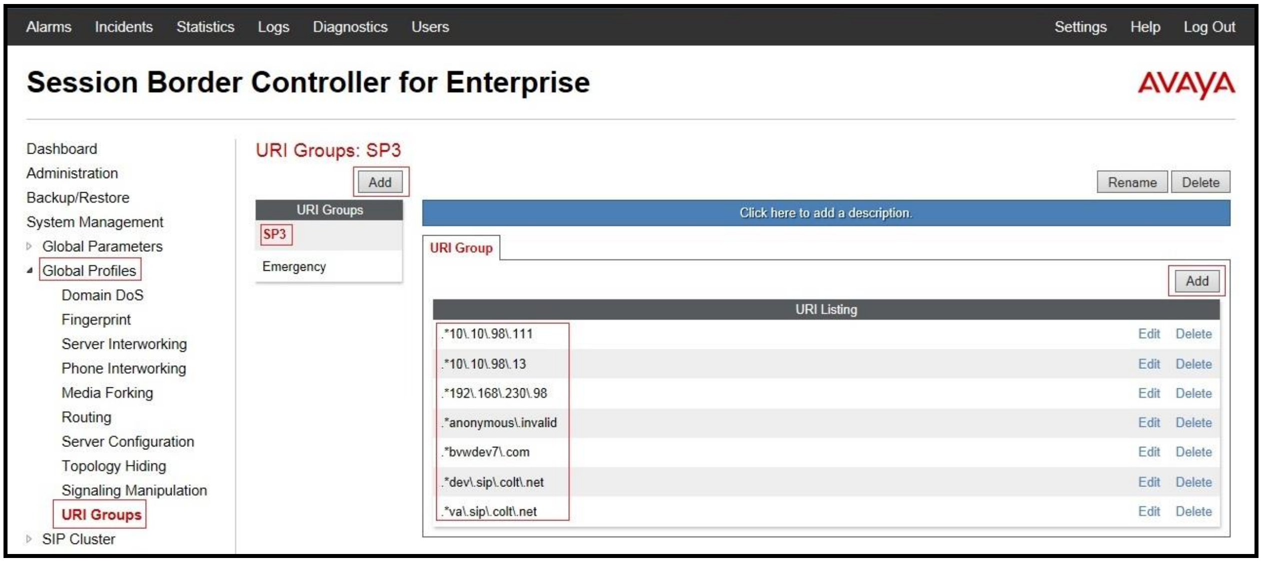
Figure 50 - Server Interworking – COLT site

7.3.3. Configure URI Groups

The URI Group feature allows administrator to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group.
The following URI Group configuration is used for this specific testing in DevConnect Lab environment. The URI-Group named **SP3** was used to match the “From” and “To” headers in a SIP call dialog received from both Enterprise and COLT service. If there is a match, the Avaya SBCE will apply the appropriate Routing profile (see **Section 7.3.4, 7.3.5**), Server Flow (see **Section 7.5.4**), and Session Flow (see **Section 7.5.5**) to route incoming and outgoing calls to the right destinations. In production environment, there is not a requirement to define this URI.

From the menu on the left-hand side, select **Global Profiles → URI Groups**. Select **Add**.

- Enter Group Name: **SP3**.
- Edit the URI Type: **Regular Expression** (not shown).
- **Add** URI: **.*10\.10\.98\.111** (Avaya SBCE public interface IP address), **.*10\.10\.98\.13** (Avaya SBCE internal interface IP address), **.*192\.168\.230\.98** (COLT Switch IP address**)**, **.*anonymous\.invalid** (Anonymous URI), **.*bvwdev7\.com** (Enterprise domain), **.*dev\.sip\.colt\.net** (Anonymous URI), **.*va\.sip\.colt\.net** (Anonymous URI**)**.
- Click **Finish** (not shown).



URI Groups: SP3

URI Listing		
.*10\.10\.98\.111	Edit	Delete
.*10\.10\.98\.13	Edit	Delete
.*192\.168\.230\.98	Edit	Delete
.*anonymous\.invalid	Edit	Delete
.*bvwdev7\.com	Edit	Delete
.*dev\.sip\.colt\.net	Edit	Delete
.*va\.sip\.colt\.net	Edit	Delete

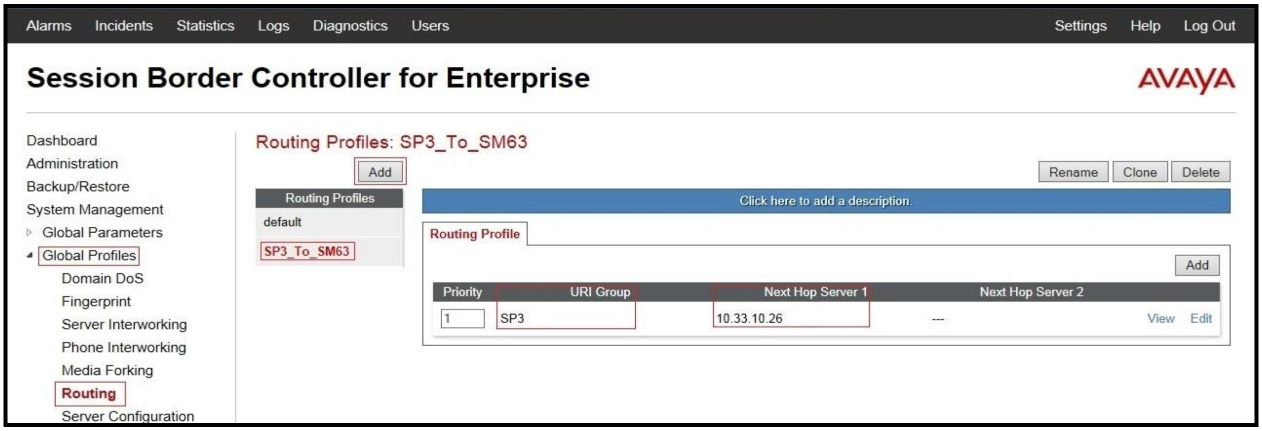
Figure 51 - URI Group

7.3.4. Configure Routing – Avaya site

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

From the menu on the left-hand side, select **Global Profiles → Routing → Add**.
Enter Profile Name: **SP3_To_SM63**.

- **URI Group**: **SP3** (See **Section 7.3.3**).
- **Next Hop Server 1**: **10.33.10.26** (Session Manager IP address).
- Check **Routing Priority based on Next Hop Server** (not shown).
- **Outgoing Transport**: **TLS** (not shown) (See **Section 6.5**).
- Click **Finish** (not shown).



Routing Profiles: SP3_To_SM63

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	SP3	10.33.10.26	---	View Edit

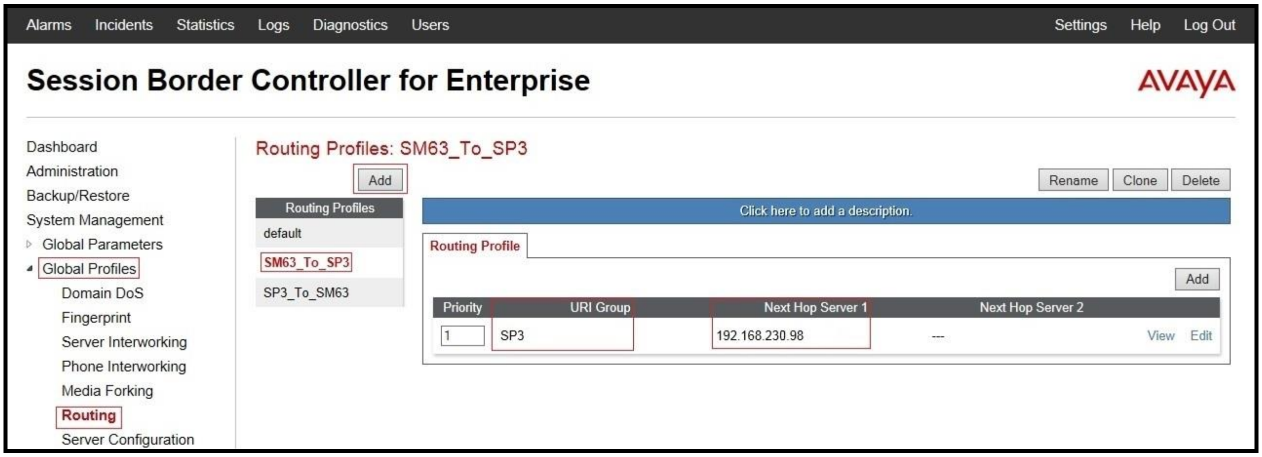
Figure 52 - Routing to Avaya

7.3.5. Configure Routing – COLT site

The Routing Profile allows administrator to manage parameters related to routing SIP signaling messages.

From the menu on the left-hand side, select **Global Profiles → Routing →Add**.
Enter Profile Name: **SM63_To_SP3**.

- **URI Group**: **SP3** (See **Section 7.3.3**).
- **Next Hop Server 1**: **192.168.230.98** (COLT Switch IP address).
- Check **Routing Priority based on Next Hop Server** (not shown).
- **Outgoing Transport** as **TLS** (not shown).
- Click **Finish** (not shown).



Routing Profiles: SM63_To_SP3

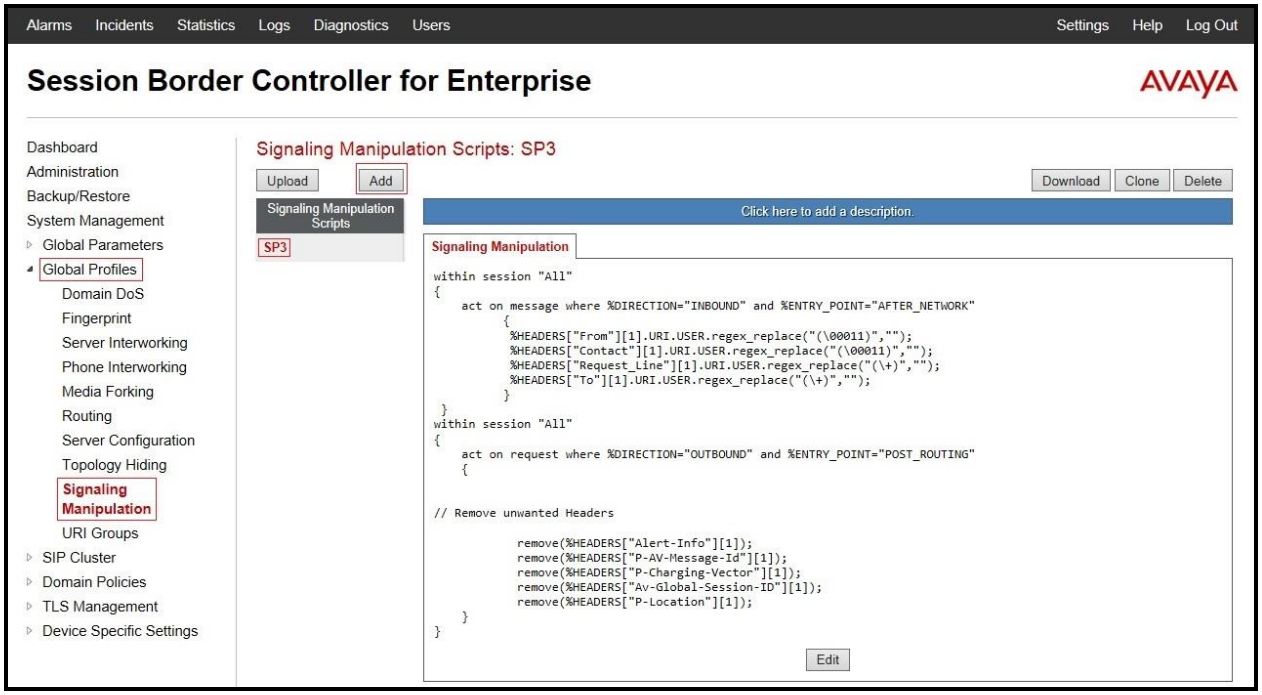
Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	SP3	192.168.230.98	---

Figure 53 - Routing to COLT

7.3.6. Configure Signaling Manipulation

The SIP signaling header manipulation feature adds the ability to add, change and delete any of the headers and other information in a SIP message.

- Select **Global Profiles** from the menu on the left-hand side.
- Select the **Signaling Manipulation**.
- Select **Add**. Enter script Title: **SP3**. In the script editing window, enter the text exactly as shown in the screenshot below to perform the following (See **Appendix 12**):
  - **Edit** script to remove unexpected prefix in From/Contact/Request_Line/To SIP Headers from incoming calls.
  - Edit the script to remove unwanted SIP Headers from outgoing calls.
  - Click Save (not shown).



```
within session "All"
{
    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
          {
           %HEADERS["From"][1].URI.USER.regex_replace("(\00011)","");
           %HEADERS["Contact"][1].URI.USER.regex_replace("(\00011)","");
           %HEADERS["Request_Line"][1].URI.USER.regex_replace("(\+)","");
           %HEADERS["To"][1].URI.USER.regex_replace("(\+)","");
          }
 }
within session "All"
{
    act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {


// Remove unwanted Headers

            remove(%HEADERS["Alert-Info"][1]);
            remove(%HEADERS["P-AV-Message-Id"][1]);
            remove(%HEADERS["P-Charging-Vector"][1]);
            remove(%HEADERS["Av-Global-Session-ID"][1]);
            remove(%HEADERS["P-Location"][1]);
    }
}
```

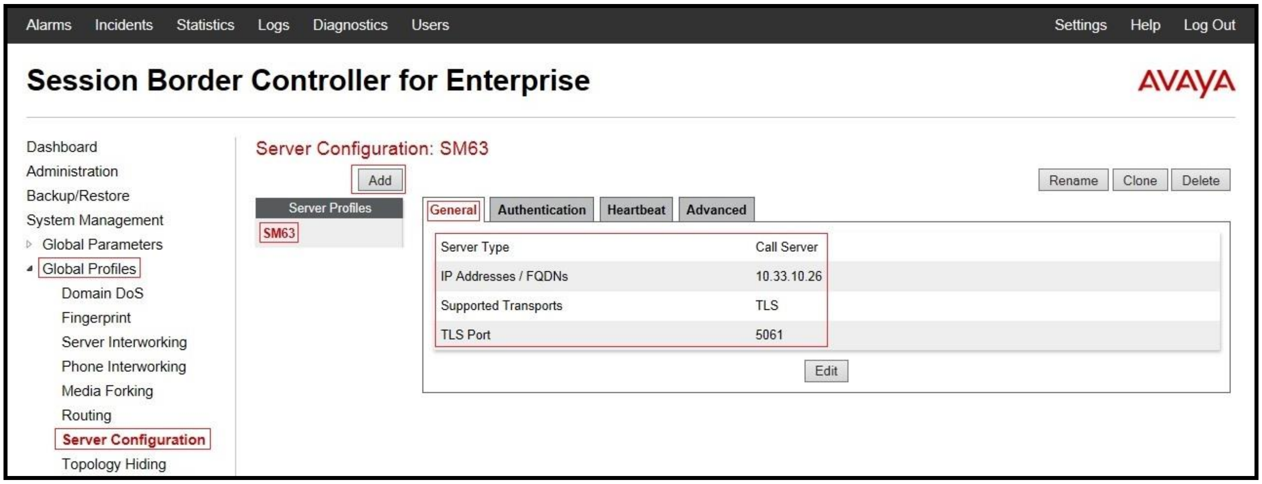
Figure 54 – Signaling Manipulation

7.3.7. Configure Server – Session Manager

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together these tabs allow the administrator to configure and manage various SIP call server-specific parameters such as TLS port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select **Global Profiles → Server Configuration →Add**. Enter profile name: **SM63**. On **General** tab, enter the following:

- **Server Type**: Select **Call Server**.
- **IP Address/FQDNs**: **10.10.33.26** (Session Manager IP Address).
- **Supported Transports**: **TLS**.
- **TLS Port**: **5061** (See **Section 6.5**).



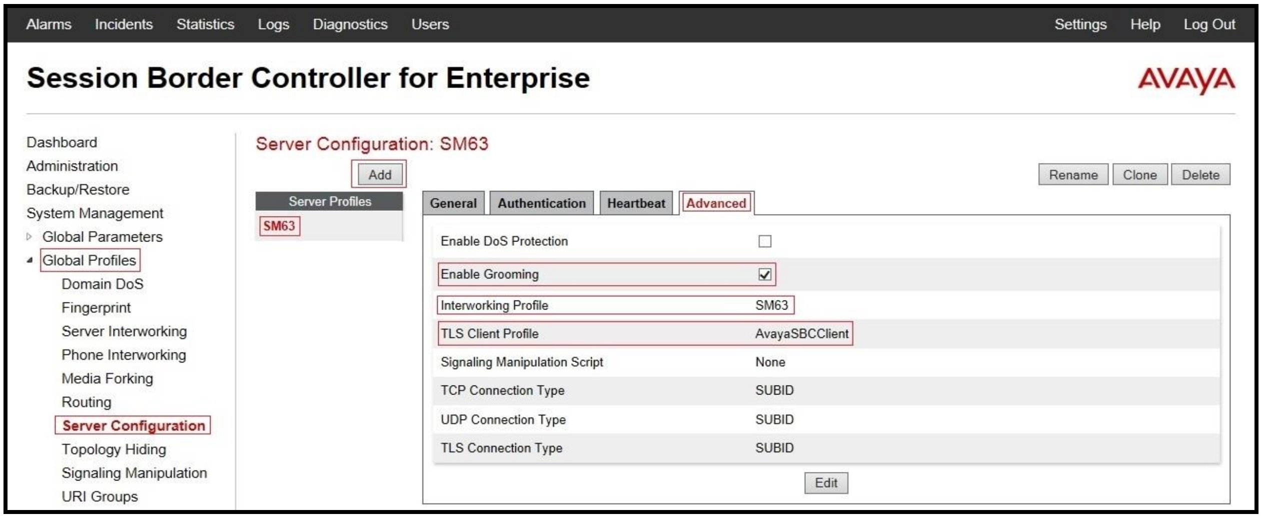
Server Configuration: SM63

Server Type	Call Server
IP Addresses / FQDNs	10.33.10.26
Supported Transports	TLS
TLS Port	5061

Figure 55 - Session Manager General Server Configuration

On the **Advanced** tab:

- Check **Enable Grooming**.
- Select **SM63** for **Interworking Profile** (See **Section 7.3.1**).
- Select **TLS Client Profile**: **AvayaSBCClient** (See **Section 7.2.2**).
- Click **Finish** (not shown).



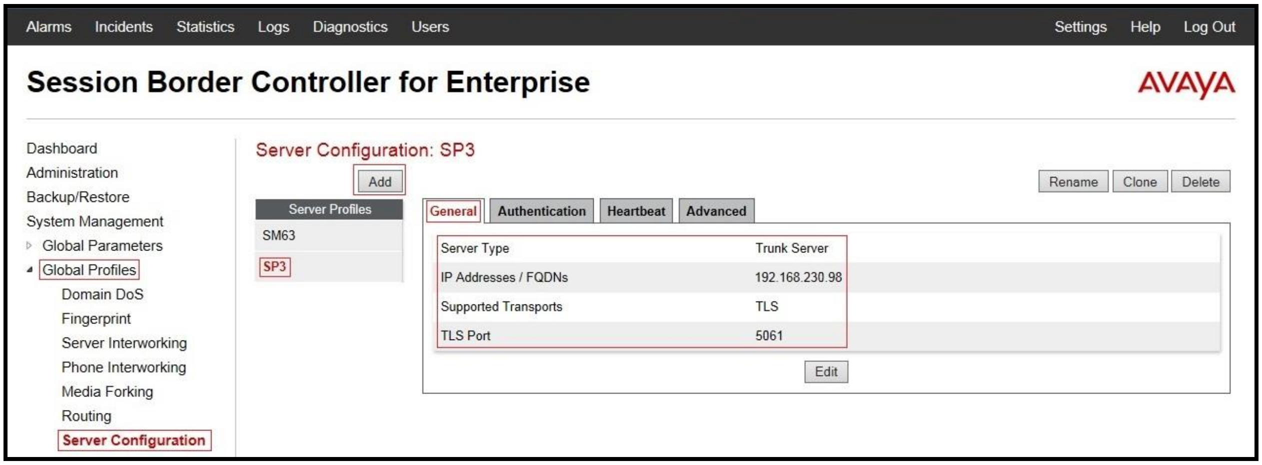
Enable DoS Protection	☐
Enable Grooming	☑
Interworking Profile	SM63
TLS Client Profile	AvayaSBCClient
Signaling Manipulation Script	None
TCP Connection Type	SUBID
UDP Connection Type	SUBID
TLS Connection Type	SUBID

Figure 56 - Session Manager Advanced Server Configuration

7.3.8. Configure Server – COLT

From the menu on the left-hand side, select **Global Profiles** → **Server Configuration** → **Add**.
Enter profile name: **SP3**.
On **General** tab, enter the following:

- **Server Type**: Select **Trunk Server**.
- **IP Address**: **192.168.230.98** (COLT Switch IP Address).
- **Supported Transports**: **TLS**.
- **TLS Port: 5061**.

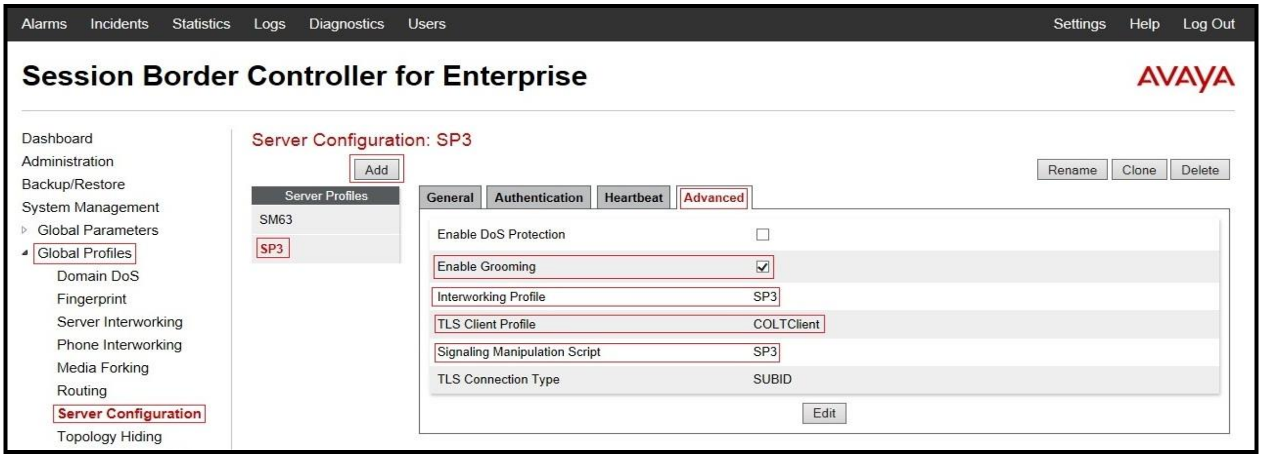


Server Type	Trunk Server
IP Addresses / FQDNs	192.168.230.98
Supported Transports	TLS
TLS Port	5061

Figure 57 - COLT General Server Configuration

On the **Advanced** tab, enter the following:

- Check **Enable Grooming**.
- **Interworking Profile**: select **SP3** (See **Section 7.3.2**).
- **TLS Client Profile**: Select **COLTClient** (See **Section 7.2.3**).
- **Signaling Manipulation Script**: Select **SP3** (See **Section 7.3.6**).
- Click **Finish** (not shown).



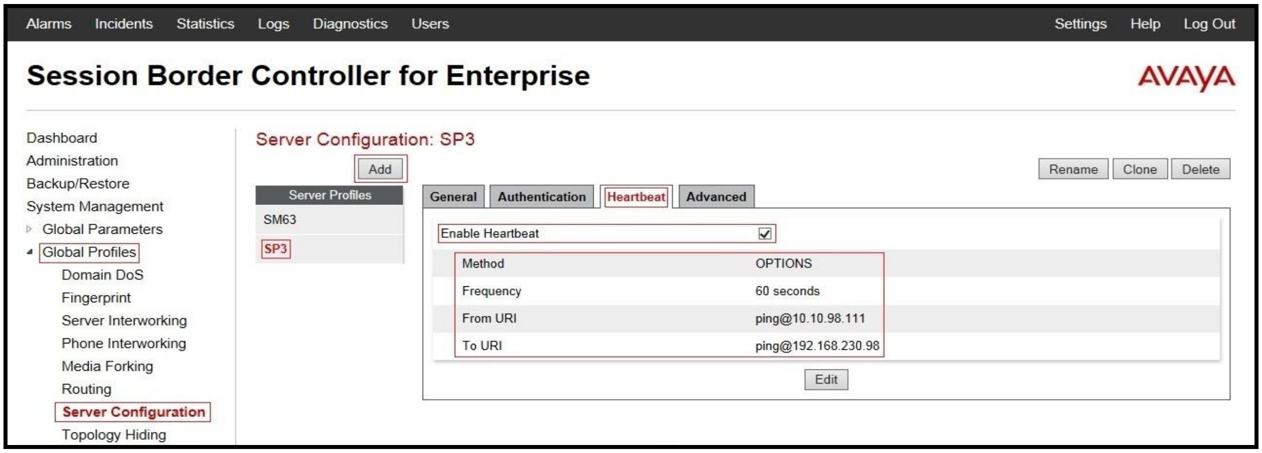
Server Configuration: SP3

Enable DoS Protection ☐
Enable Grooming ☑
Interworking Profile SP3
TLS Client Profile COLTClient
Signaling Manipulation Script SP3
TLS Connection Type SUBID

Figure 58 - COLT Advanced Server Configuration

On the **Heartbeat** tab, enter the following:

- Check **Enable Heartbeat**.
- Select **Method**: **OPTIONS**.
- Enter **Frequency**: **60 seconds**.
- Enter **From URI**: **ping@10.10.98.111**.
- Enter **To URI**: **ping@192.168.230.98**.
- Click **Finish** (not shown).



Server Configuration: SP3

Enable Heartbeat ☑
Method OPTIONS
Frequency 60 seconds
From URI ping@10.10.98.111
To URI ping@192.168.230.98

Figure 59 - COLT Heartbeat Server Configuration

7.3.9. Configure Topology Hiding – Avaya site

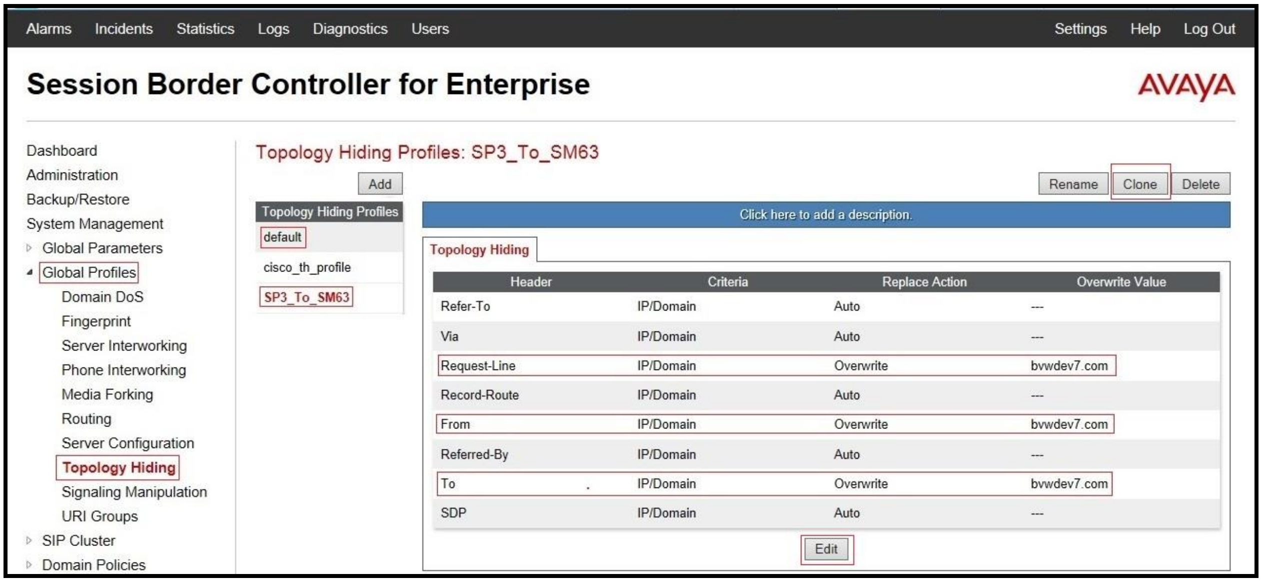
The **Topology Hiding** screen allows administrator to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

From the menu on the left-hand side, select **Global Profiles → Topology Hiding**.

Select **default** under **Topology Hiding Profiles**, and click **Clone**. Enter **Clone Name**: **SP3_To_SM63**. Click **Finish** (not shown).

Select **SP3_To_SM63** under **Topology Hiding Profiles**, and click **Edit**

- For the Header **Request-Line,**
    - In the **Criteria** column select **IP/Domain**
    - In the **Replace Action** column select: **Overwrite**
    - In the **Overwrite Value** column: **bvwdev7.com**
- For the Header **From,**
    - In the **Criteria** column select **IP/Domain**
    - In the **Replace Action** column select: **Overwrite**
    - In the **Overwrite Value** column: **bvwdev7.com**
- For the Header **To,**
    - In the **Criteria** column select **IP/Domain**
    - In the **Replace Action** column select: **Overwrite**
    - In the **Overwrite Value** column: **bvwdev7.com**
- Click **Finish** (not shown).



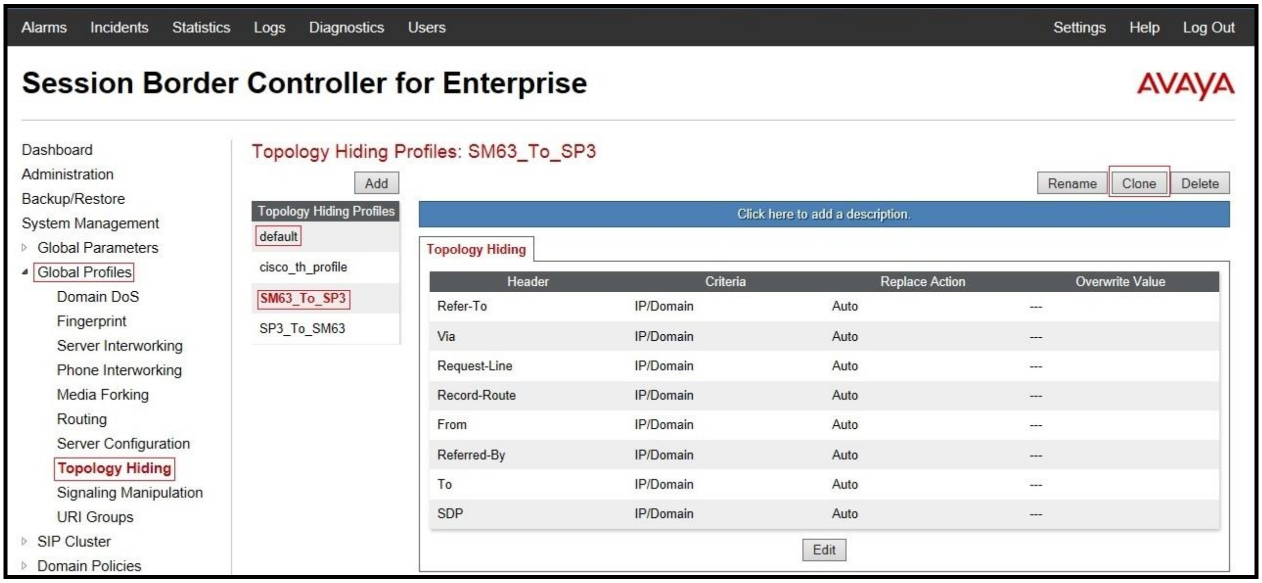
Header	Criteria	Replace Action	Overwrite Value
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	bvwdev7.com
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	bvwdev7.com
Referred-By	IP/Domain	Auto	---
To	IP/Domain	Overwrite	bvwdev7.com
SDP	IP/Domain	Auto	---

Figure 60 - Topology Hiding Session Manager

7.3.10. Configure Topology Hiding – COLT site

From the menu on the left-hand side, select **Global Profiles** → **Topology Hiding**.

Select **default** under **Topology Hiding Profiles**, and click **Clone**. Enter **Clone Name**: **SM63_To_SP3**. Click **Finish** (not shown).



Topology Hiding Profiles: SM63_To_SP3

Header	Criteria	Replace Action	Overwrite Value
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
To	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---

Figure 61 - Topology Hiding COLT

7.4. Domain Policies

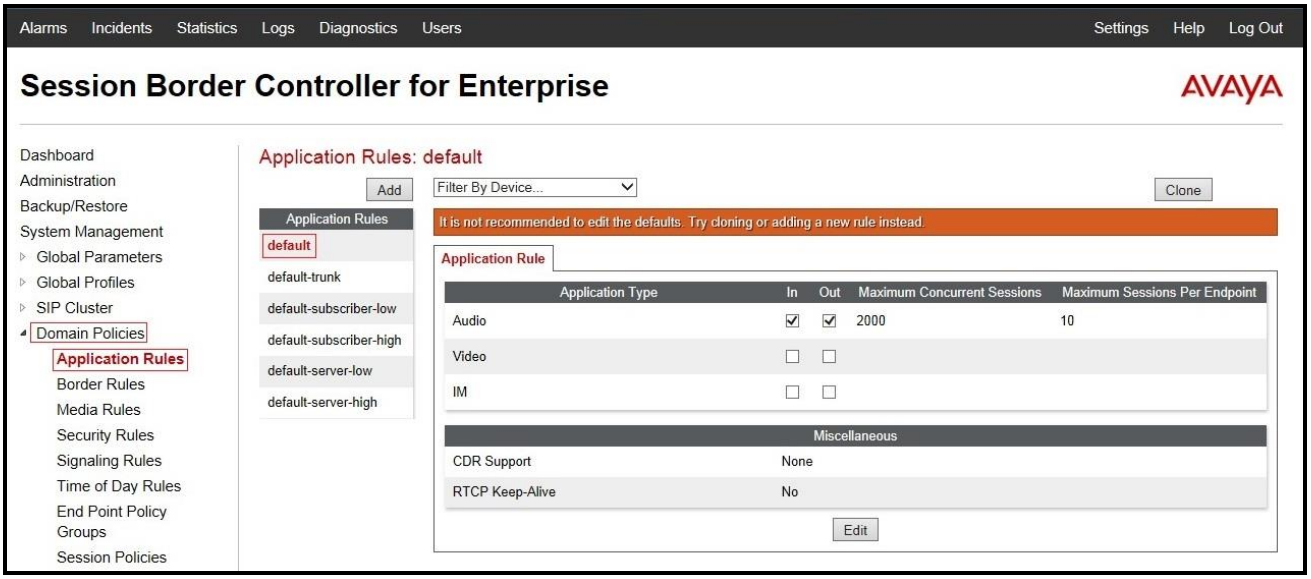
The Domain Policies feature allows administrator to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or an administrator can create a custom domain policy.

7.4.1. Create Application Rules

Application Rules allow one to define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, one can determine the maximum number of concurrent voice and video sessions so that the network will process to prevent resource exhaustion. For the compliance test, the predefined **default** application rule (shown below) was used for both Session Manager and the COLT server.

From the menu on the left-hand side, select **Domain Policies → Application Rules**.

- Select the **default** rule to view.



It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	☑	☑	2000	10
Video	☐	☐		
IM	☐	☐		

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

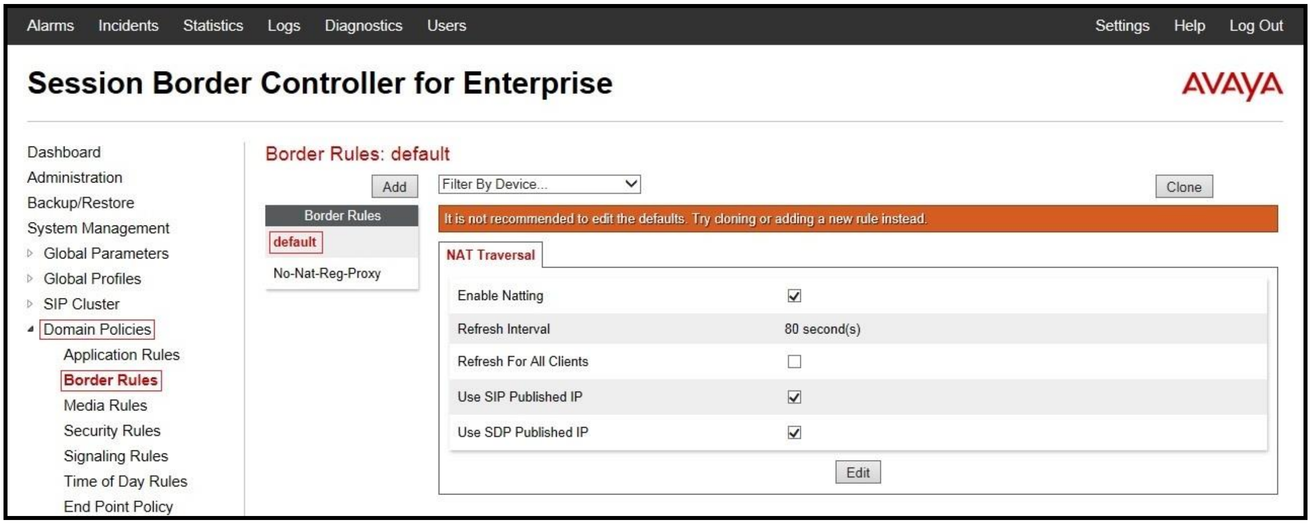
Figure 62 – Application Rule

7.4.2. Create Border Rules

Border Rules allow one to control NAT Traversal. The NAT Traversal feature allows one to determine whether or not call-flow through the DMZ needs to traverse a firewall and the manner in which pinholes will be kept open in the firewall to accommodate traffic. For the compliance test, the predefined **default** border rule (shown below) was used for both Session Manager and the COLT server.

From the menu on the left-hand side, select **Domain Policies →Border Rules**.

- Select the **default** Rule to view.



It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Enable Natting	☑
Refresh Interval	80 second(s)
Refresh For All Clients	☐
Use SIP Published IP	☑
Use SDP Published IP	☑

Figure 63 – Border Rule

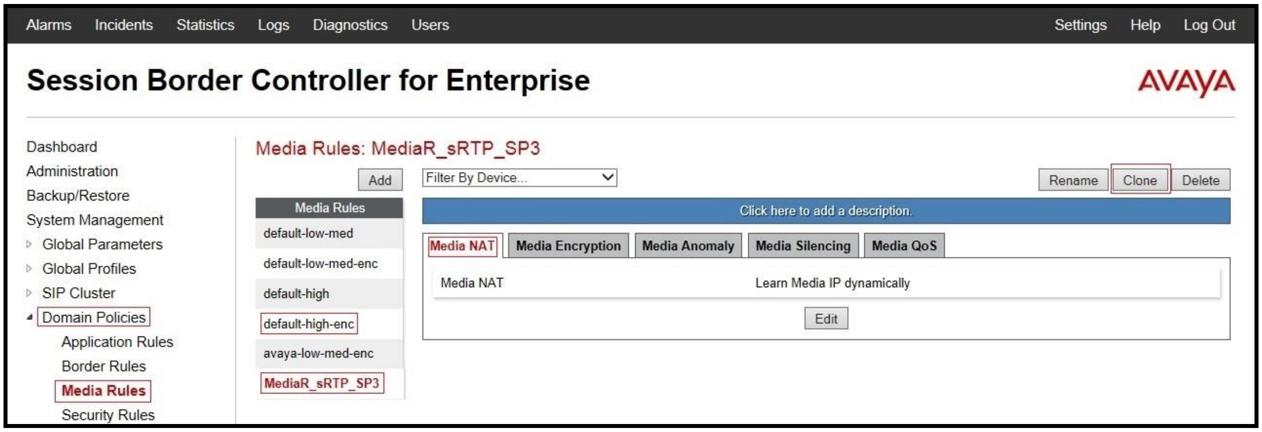
7.4.3. Create Media Rules

Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, the predefined **default-high-enc** media rule (shown below) was used to clone for both Session Manager and the COLT server.

From the menu on the left-hand side, select **Domain Policies → Media Rules**.

- Select the **default-high-enc** rule, click **Clone**. Enter **Clone Name**: **MediaR_sRTP_SP3**. Click **Finish** (not shown).
- Select **MediaR_sRTP_SP3** under Media Rules to **Edit**.

The **Media NAT** tab has no entries.

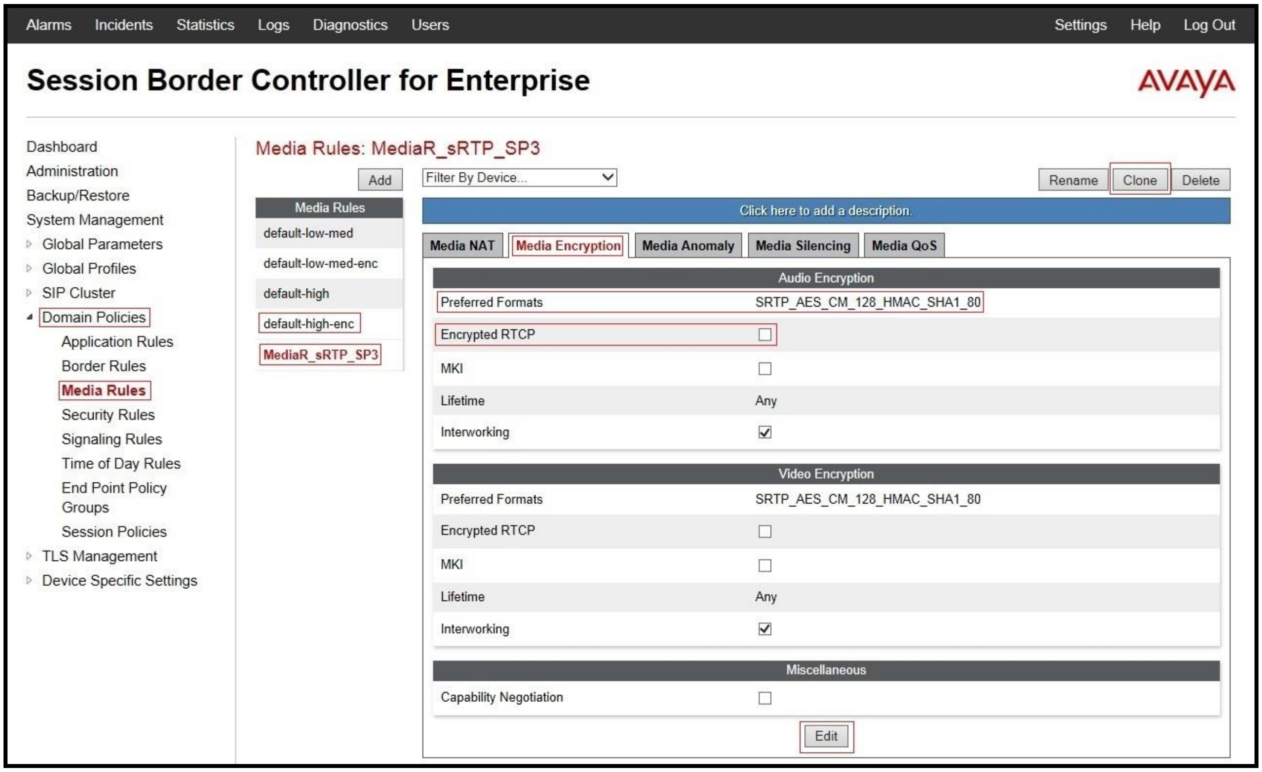


Media Rules: MediaR_sRTP_SP3

Media NAT	Learn Media IP dynamically

Figure 64 – Media Rule

The **Media Encryption** tab indicates that **SRTP_AES_CM_128_HMAC_SHA1_80** encryption was used. Make sure to uncheck **Encrypted RTCP**.



Media Rules: MediaR_sRTP_SP3

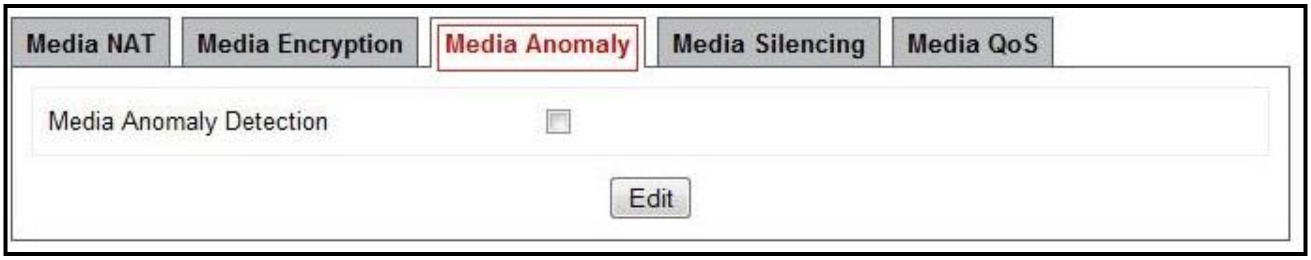
Audio Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80
Encrypted RTCP	☐
MKI	☐
Lifetime	Any
Interworking	☑

Video Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80
Encrypted RTCP	☐
MKI	☐
Lifetime	Any
Interworking	☑

Miscellaneous	
Capability Negotiation	☐

Figure 65 – Media Rule - Encryption

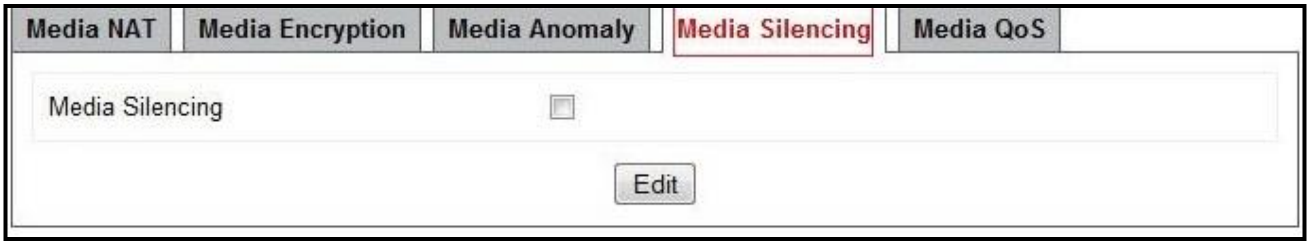
The **Media Anomaly** tab shows **Media Anomaly Detection** was disabled.



Media Anomaly Detection ☐

Figure 66 – Media Rule - Anomaly

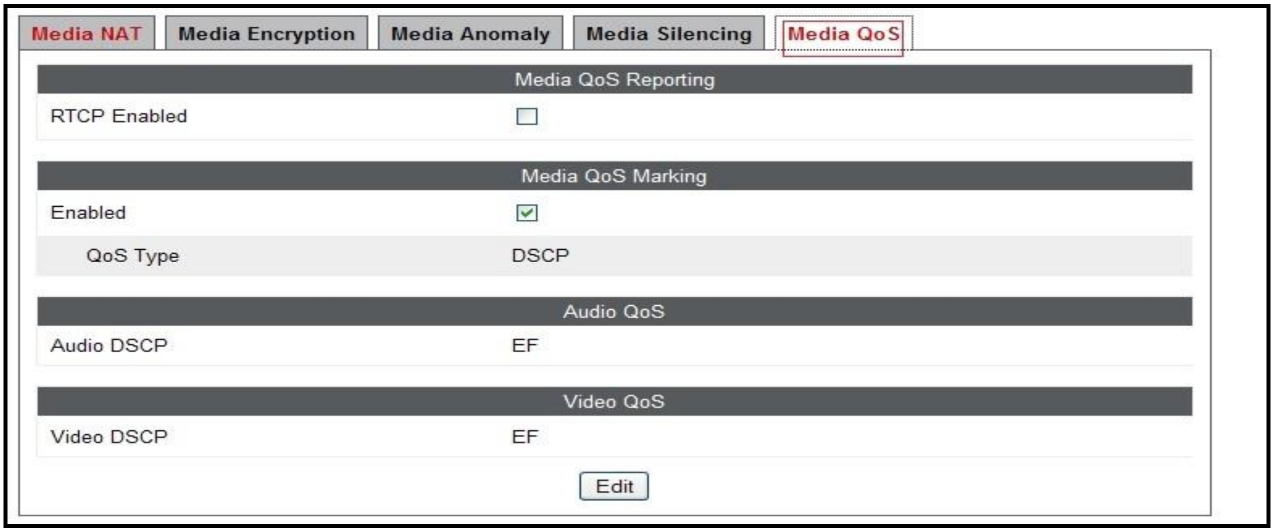
The **Media Silencing** tab shows **Media Silencing** was disabled.



Media Silencing ☐

Figure 67 – Media Rule - Silencing

The **Media QoS** settings are shown below.



Media QoS Reporting

RTCP Enabled ☐

Media QoS Marking

Enabled ☑

QoS Type DSCP

Audio QoS

Audio DSCP EF

Video QoS

Video DSCP EF

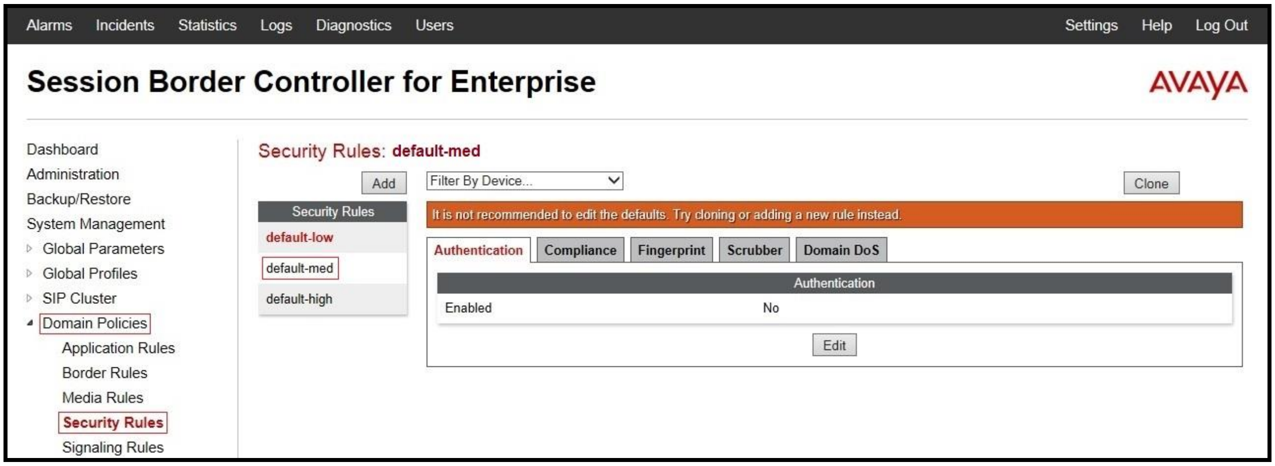
Figure 68 – Media Rule - QoS

7.4.4. Create Security Rules

Security Rules allow one to define which enterprise-wide VoIP and Instant Message (IM) security features will be applied to a particular call flow. Security Rules allows one to configure Authentication, Compliance, Fingerprinting, Scrubber, and Domain DoS. In addition to determining which combination of security features are applied, one can also define the security feature profile, so that the feature is applied in a specific manner to a specific situation. For the compliance test, the predefined **default-med** security rule (shown below) was used for both Session Manager and the COLT server.

From the menu on the left-hand side, select **Domain Policies → Security Rules**.

- Select the **default-med** rule to view.



It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Authentication	
Enabled	No

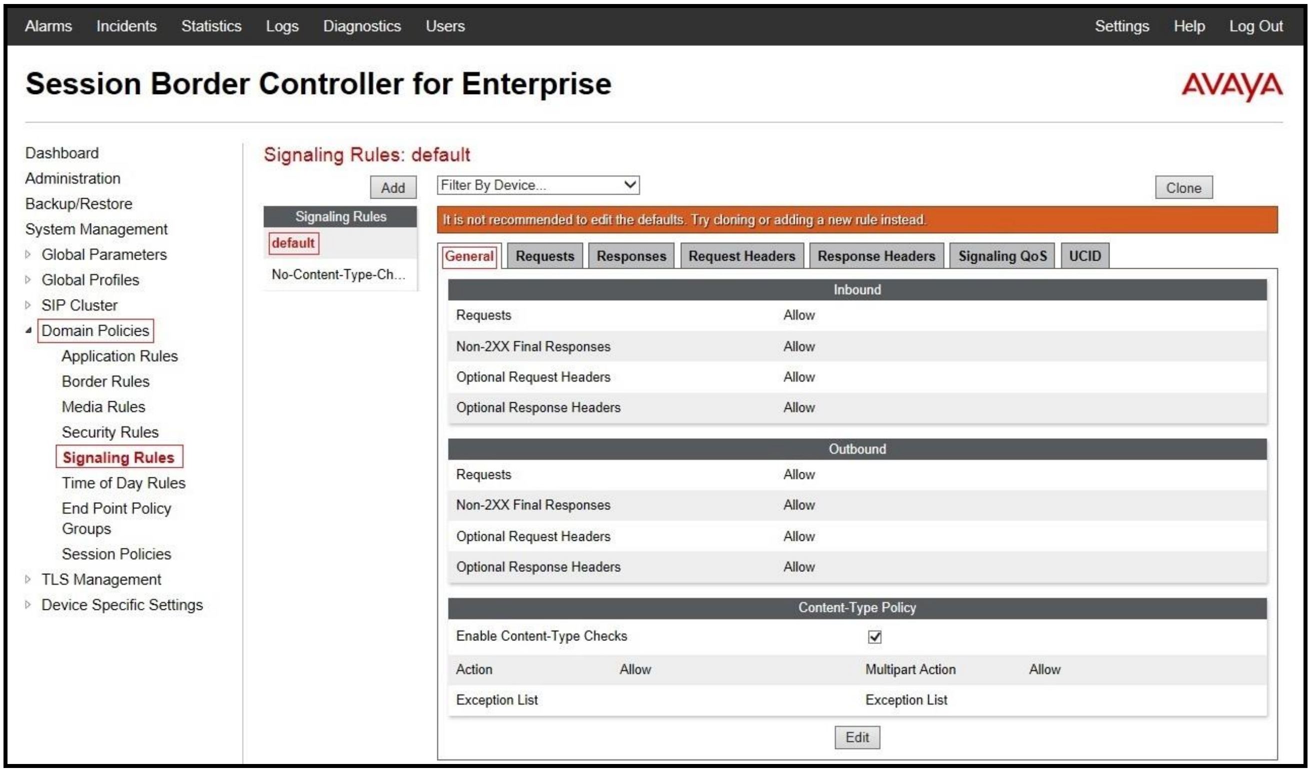
Figure 69 – Security Rule

7.4.5. Create Signaling Rules

Signaling Rules allow one to define the action to be taken, (Allow, Block, Block with Response, etc.), for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they are parsed and “pattern matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching. For the compliance test, the predefined **default** signaling rule (shown below) was used for both Session Manager and the COLT server.

From the menu on the left-hand side, select **Domain Policies → Signaling Rules**.

- Select the **default** rule to view.



Signaling Rules: default

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

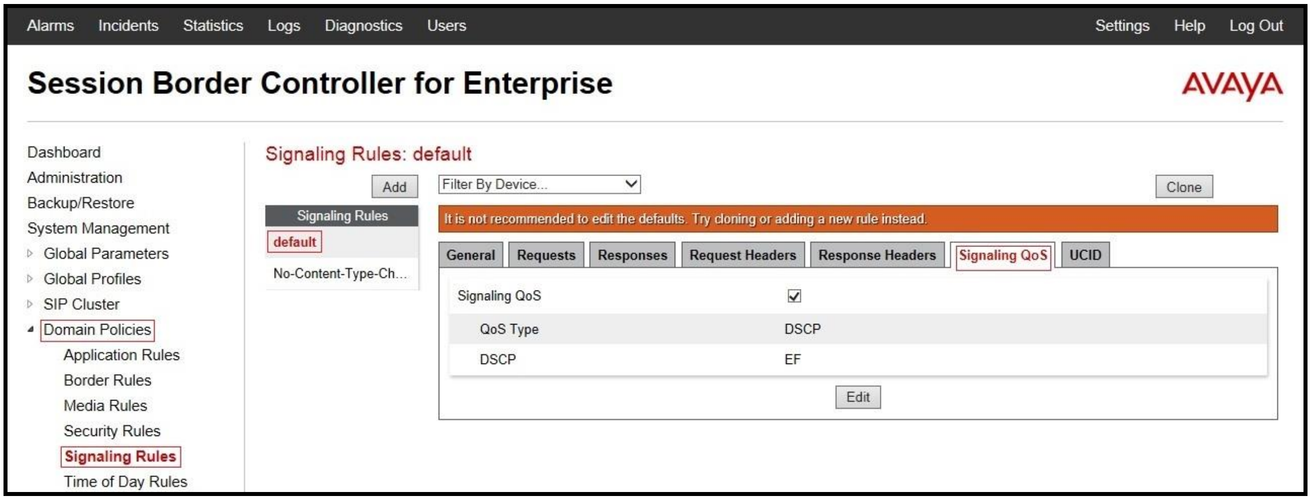
Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy			
Enable Content-Type Checks		☑	
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

Figure 70 – Signaling Rule

The **Requests**, **Responses**, **Request Headers**, **Response Headers** and **UCID** tabs have no entries.

The **Signaling QoS** tab is shown below.



Signaling Rules: default

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Signaling QoS	☑
QoS Type	DSCP
DSCP	EF

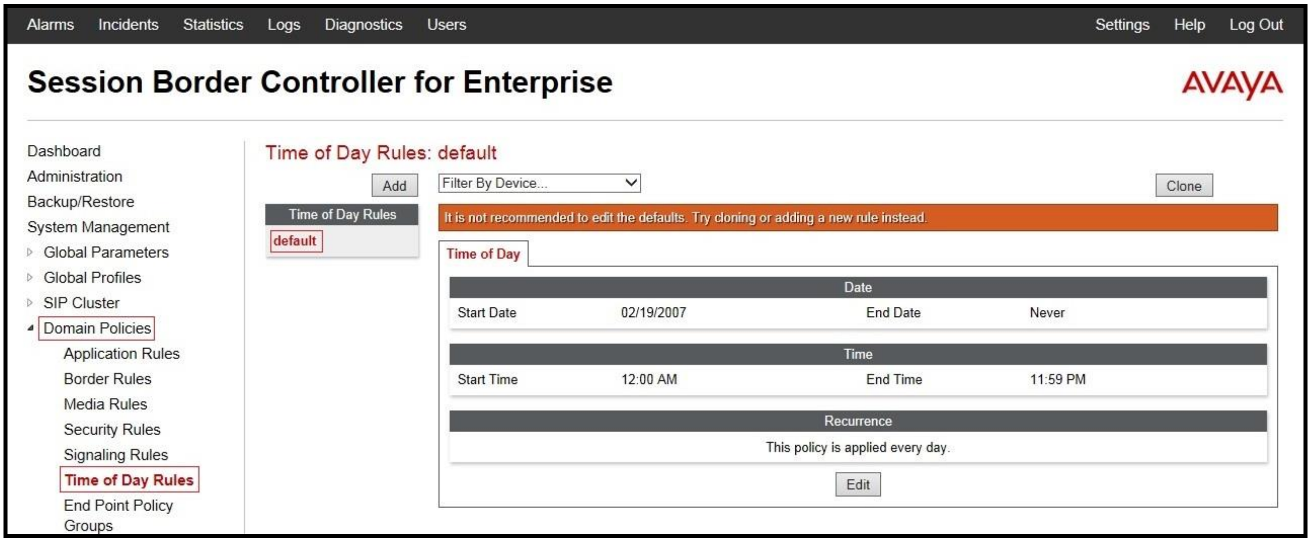
Figure 71 – Signaling Rule - QoS

7.4.6. Create Time of Day Rules

A Time-of-day (ToD) Rule allows one to determine when the domain policy which is assigned to will be in effect. ToD rules provide complete flexibility to fully accommodate the enterprise by, not only determining when a particular domain policy will be in effect, but also to whom it will apply, and for how long it will remain in effect. For the compliance test, the predefined default Time of Day rule (shown below) was used for both Session Manager and the COLT server.

From the menu on the left-hand side, select **Domain Policies → Time of Day Rules**.

- Select the **default** rule to view.



Time of Day Rules: default

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Date

Start Date	02/19/2007	End Date	Never

Time

Start Time	12:00 AM	End Time	11:59 PM

Recurrence

This policy is applied every day.

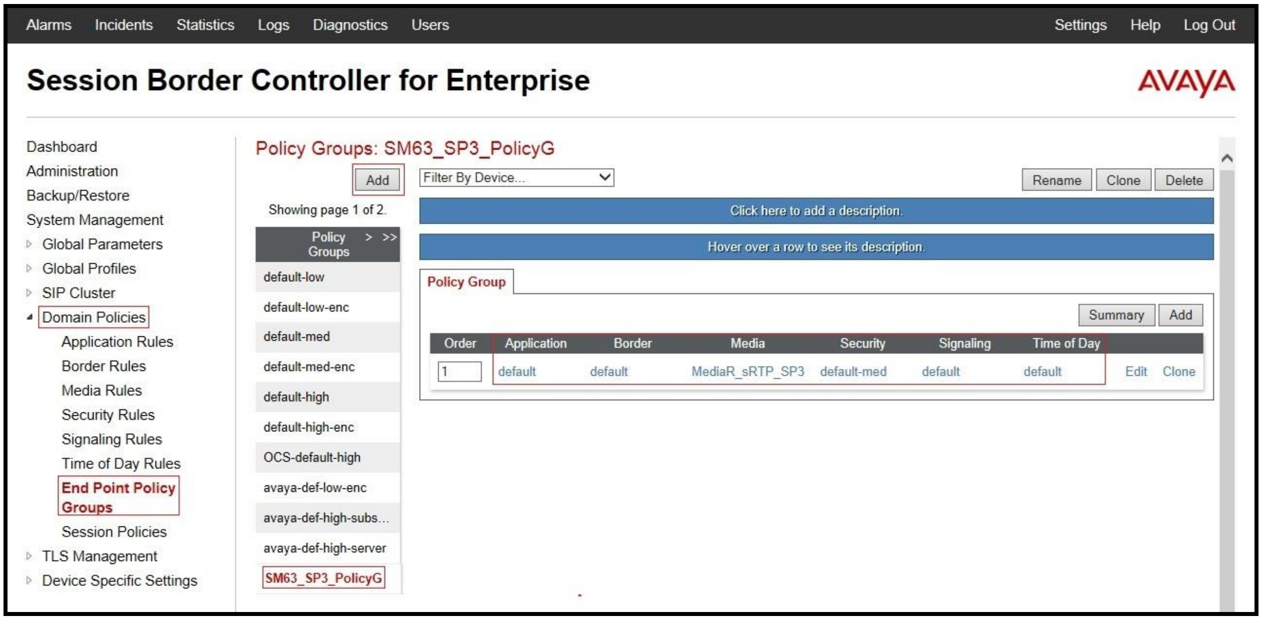
Figure 72 – Time of Day Rule

7.4.7. Create Endpoint Policy Groups

The End-Point Policy Group feature allows one to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, and ToD, each of which was created using the procedures contained in the previous sections. A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of Avaya SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**.

- Select **Add**.
- Enter **Group Name**: **SM63_SP3_PolicyG**.
  - **Application Rule**: **default**
  - **Border Rule**: **default**
  - **Media Rule**: **MediaR_sRTP_SP3**
  - **Security Rule**: **default-med**
  - **Signaling Rule**: **default**
  - **Time of Day**: **default**
- Select **Finish** (not shown).

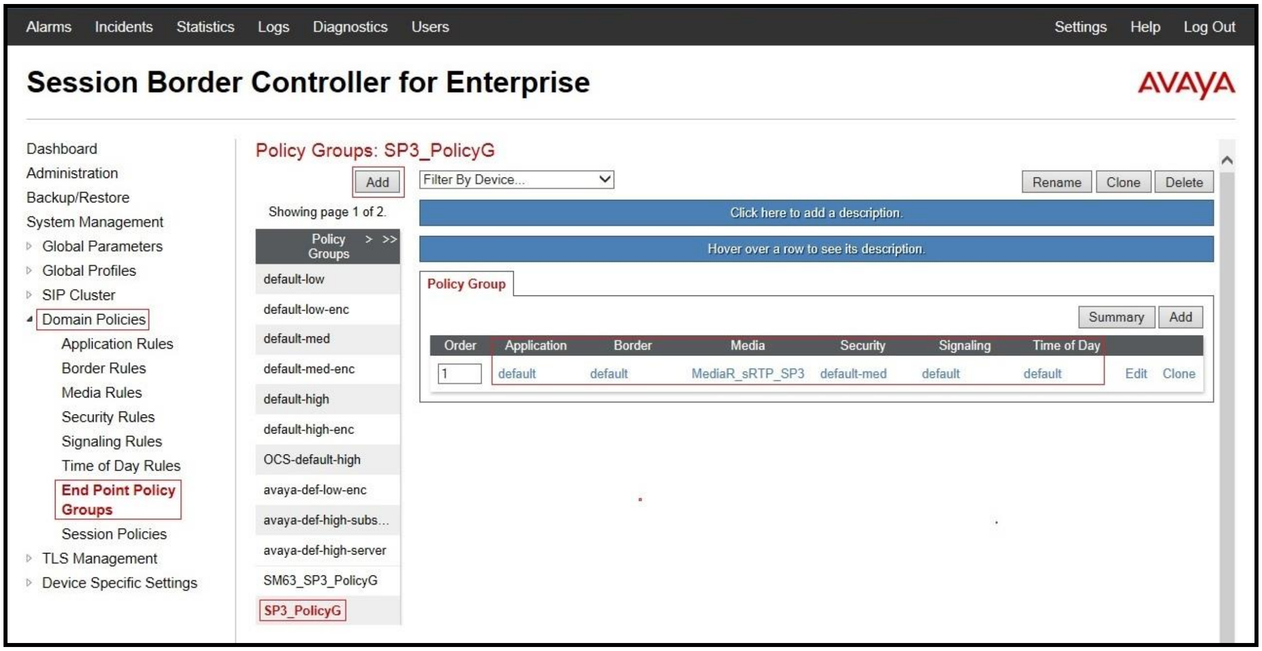


Order	Application	Border	Media	Security	Signaling	Time of Day
1	default	default	MediaR_sRTP_SP3	default-med	default	default

Figure 73 – Session Manager End Point Policy

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**.

- Select **Add**.
- Enter **Group Name**: **SP3_PolicyG**.
  - **Application Rule**: **default**
  - **Border Rule**: **default**
  - **Media Rule**: **MediaR_sRTP_SP3**
  - **Security Rule**: **default-med**
  - **Signaling Rule**: **default**
  - **Time of Day**: **default**
- Select **Finish** (not shown).



Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default	default	MediaR_sRTP_SP3	default-med	default	default	Edit	Clone

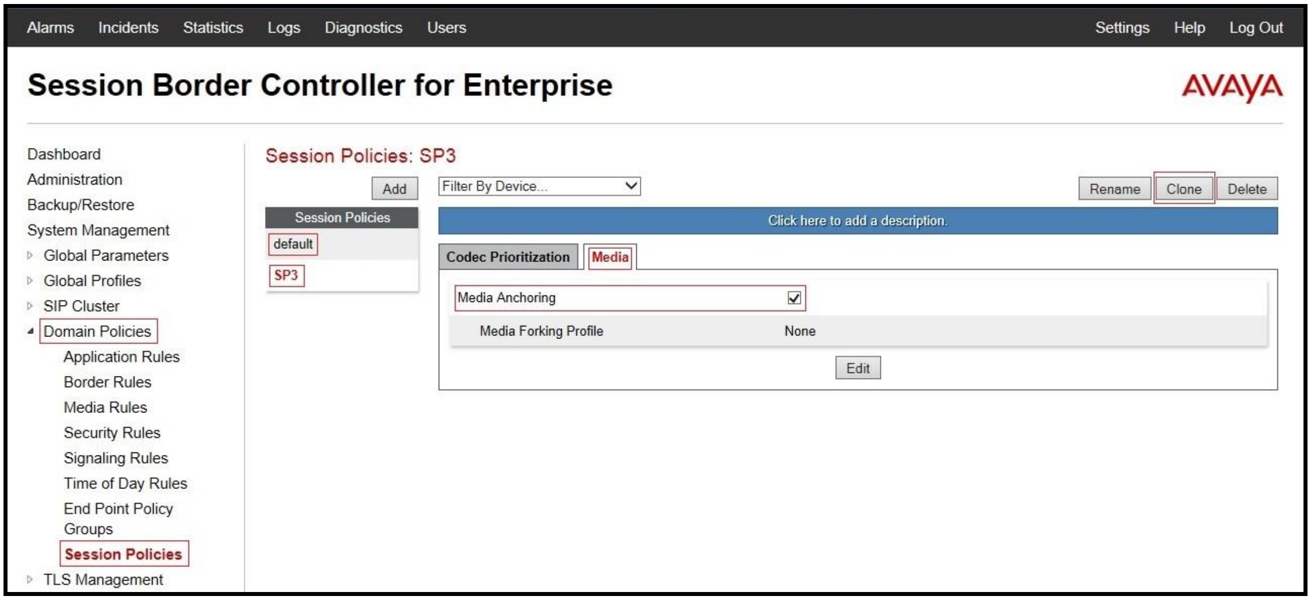
Figure 74 – COLT End Point Policy

7.4.8. Create Session Policy

Session Policies allow users to define RTP media packet parameters such as codec types (audio and video) and codec matching priority. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

From the menu on the left-hand side, select **Domain Policies** → **Session Policies**.

- Select the **default** policy.
- Select **Clone** button.
  - Enter **Clone Name**: **SP3**.
  - Click **Finish** (not shown).
- Click **Edit** button on **Media** tab.
  - Check **Media Anchoring**.
  - Select **Finish** (not shown).



Media Anchoring ☑

Media Forking Profile None

Figure 75 - Session Policy

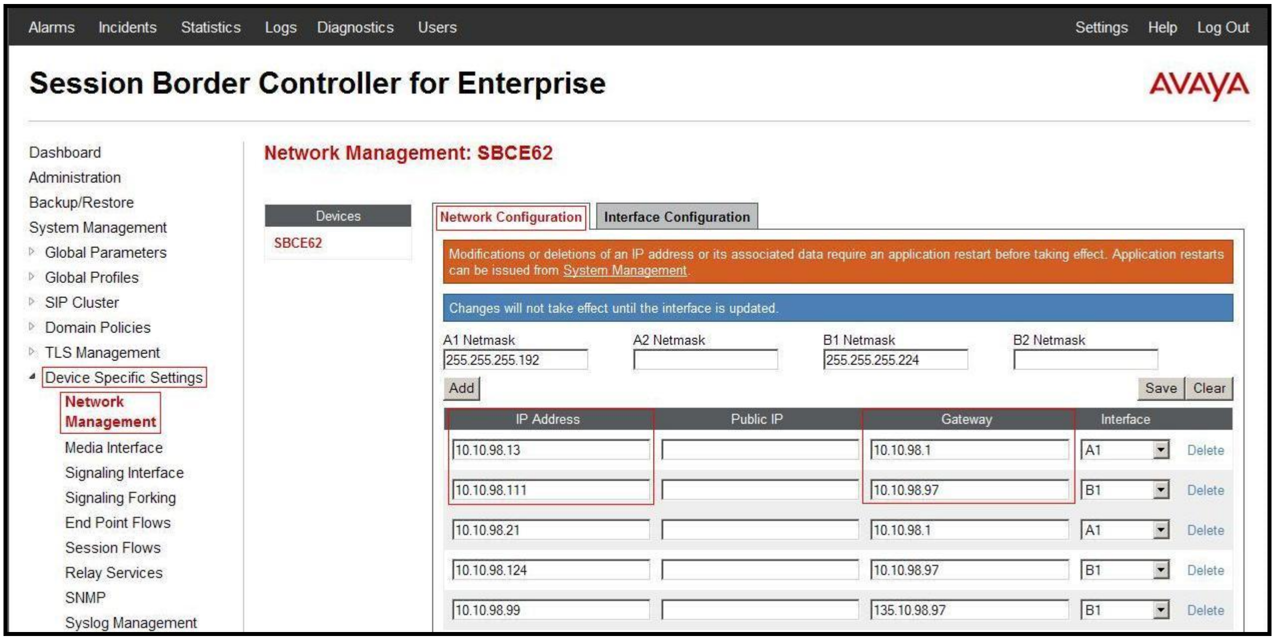
7.5. Device Specific Settings

The Device Specific Settings feature for SIP allows one to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, one has the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

7.5.1. Manage Network Settings

From the menu on the left-hand side, select **Device Specific Settings → Network Management**.

- Enter the **IP Address** and **Gateway Address** for both the Inside and the Outside interfaces:
    - **IP Address** for Inside interface: **10.10.98.13**; **Gateway**: **10.10.98.1**.
    - **IP Address** for Outside interface: **10.10.98.111**; **Gateway**: **10.10.98.97**.
- Select the physical interface used in the Interface column:
    - **Inside Interface**: **A1**.
    - **Outside Interface**: **B1**.



Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

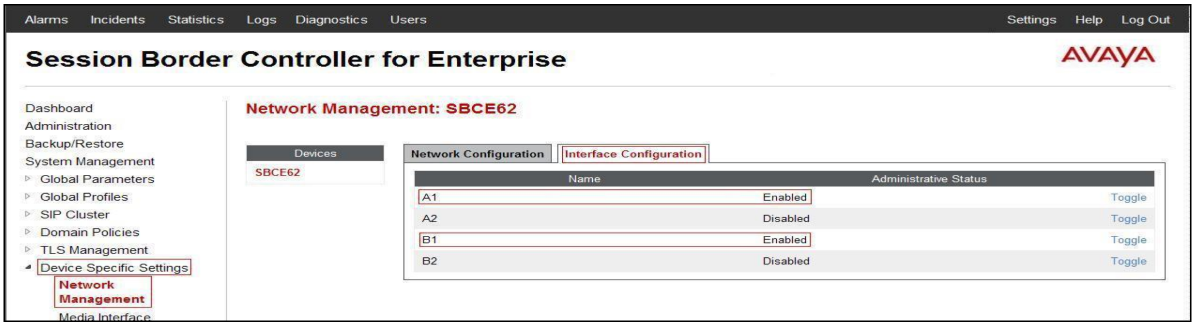
Changes will not take effect until the interface is updated.

A1 Netmask: 255.255.255.192
A2 Netmask:
B1 Netmask: 255.255.255.224
B2 Netmask:

IP Address	Public IP	Gateway	Interface	
10.10.98.13		10.10.98.1	A1	Delete
10.10.98.111		10.10.98.97	B1	Delete
10.10.98.21		10.10.98.1	A1	Delete
10.10.98.124		10.10.98.97	B1	Delete
10.10.98.99		135.10.98.97	B1	Delete

Figure 76 - Network Management

- Select the **Interface Configuration** tab.
- Toggle the state of the physical interfaces being used to **Enabled**.



Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

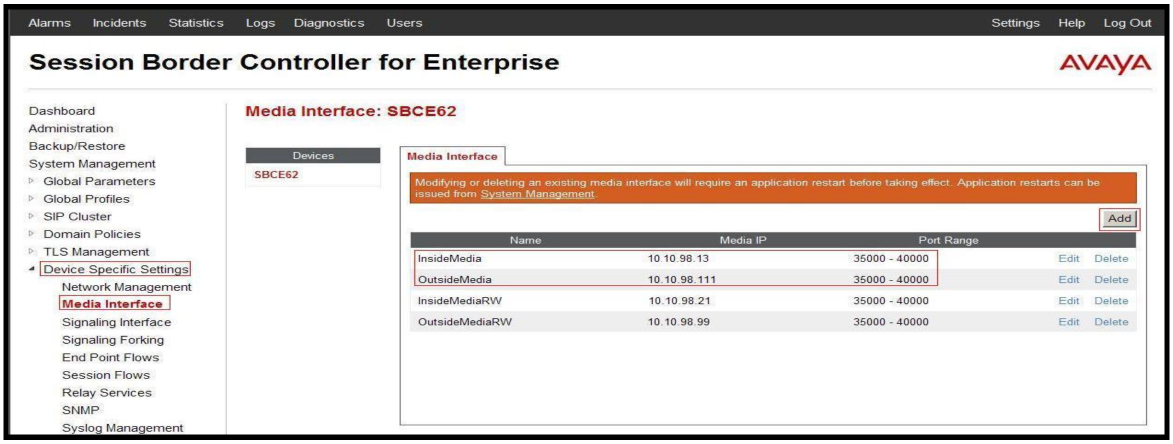
Figure 77 - Network Interface Status

7.5.2. Create Media Interfaces

Media Interfaces define the type of signaling on the ports. The default media port range on the Avaya can be used for both inside and outside ports.

From the menu on the left-hand side, **Device Specific Settings → Media Interface**.

- Select **Add**.
  - **Name**: **InsideMedia**.
  - **Media IP**: **10.10.98.13** (Internal IP Address toward Session Manager SIP trunk).
  - **Port Range**: **35000 – 40000**.
  - Click **Finish** (not shown).
- Select **Add**.
  - **Name**: **OutsideMedia**.
  - **Media IP**: **10.10.98.111** (External IP Address toward COLT SIP trunk).
  - **Port Range**: **35000 – 40000**.
  - Click **Finish** (not shown).



Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Media IP	Port Range		
InsideMedia	10.10.98.13	35000 - 40000	Edit	Delete
OutsideMedia	10.10.98.111	35000 - 40000	Edit	Delete
InsideMediaRW	10.10.98.21	35000 - 40000	Edit	Delete
OutsideMediaRW	10.10.98.99	35000 - 40000	Edit	Delete

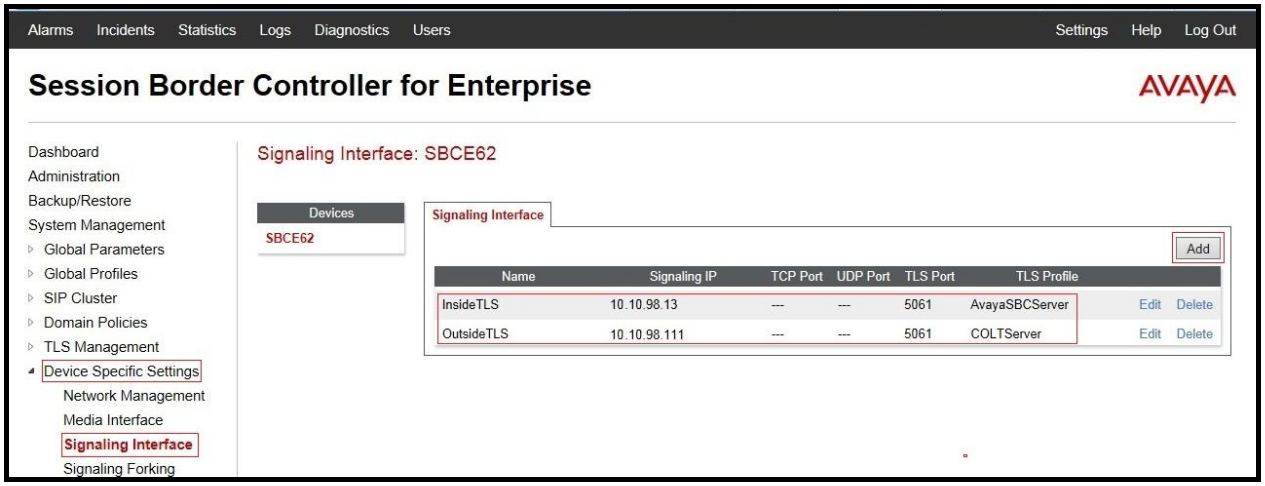
Figure 78 - Media Interface

7.5.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

From the menu on the left-hand side, select **Device Specific Settings** → **Signaling Interface**.

- Select **Add**.
  - **Name**: **InsideTLS**.
  - **Media IP**: **10.10.98.13** (Internal IP Address toward Session Manager SIP trunk).
  - **TLS Port**: **5061**.
  - **TLS Profile**: **AvayaSBCServer** (See **Section 7.2.4**).
  - Click **Finish** (not shown).
- Select **Add**.
  - **Name**: **OutsideTLS**.
  - **Media IP**: **10.10.98.111** (External IP Address toward COLT SIP trunk).
  - **TLS Port**: **5061**.
  - **TLS Profile**: **COLTServer** (See **Section 7.2.5**).
  - Click **Finish** (not shown).



Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
InsideTLS	10.10.98.13	---	---	5061	AvayaSBCServer	Edit Delete
OutsideTLS	10.10.98.111	---	---	5061	COLTServer	Edit Delete

Figure 79 - Signaling Interface

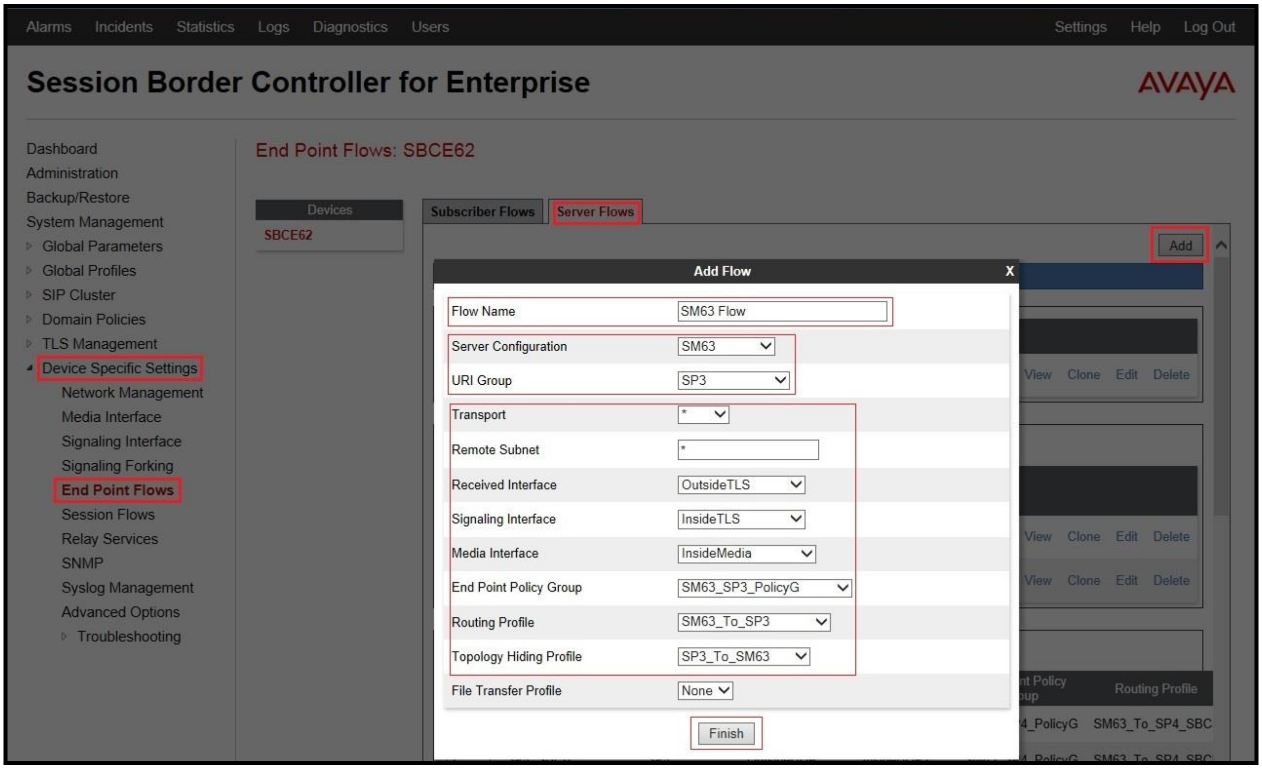
7.5.4. Configuration Server Flows

Server Flows allow administrator to categorize trunk-side signaling and apply a policy.

7.5.4.1 Create End Point Flows – SM63 Flow

From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**.

- Select the **Server Flows** tab.
- Select **Add**, enter **Flow Name**: **SM63 Flow**.
  - **Server Configuration**: **SM63**.
  - **URI Group**: **SP3**.
  - **Transport: ***.
  - **Remote Subnet: ***.
  - **Received Interface**: **OutsideTLS**.
  - **Signaling Interface**: **InsideTLS**.
  - **Media Interface**: **InsideMedia**.
  - **End Point Policy Group**: **SM63_SP3_PolicyG**.
  - **Routing Profile**: **SM63_To_SP3**.
  - **Topology Hiding Profile**: **SP3_To_SM63**.
  - Click **Finish**.



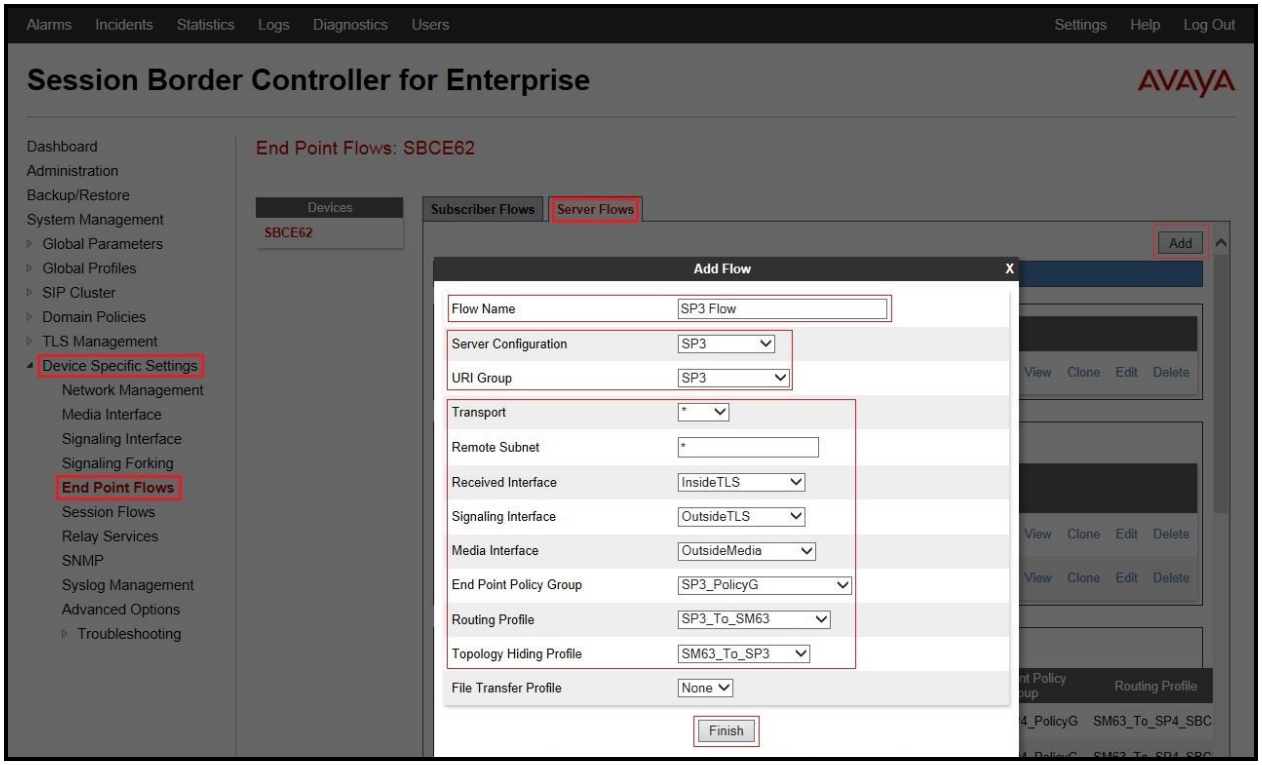
Flow Name	SM63 Flow
Server Configuration	SM63
URI Group	SP3
Transport	*
Remote Subnet	*
Received Interface	OutsideTLS
Signaling Interface	InsideTLS
Media Interface	InsideMedia
End Point Policy Group	SM63_SP3_PolicyG
Routing Profile	SM63_To_SP3
Topology Hiding Profile	SP3_To_SM63
File Transfer Profile	None

Figure 80 - End Point Flow – SM Server Flow

7.5.4.2 Create End Point Flows – COLT Flow

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**.

- Select the **Server Flows** tab.
- Select **Add**, enter **Flow Name**: **SP3 Flow**.
  - **Server Configuration**: **SP3**.
  - **URI Group**: **SP3**.
  - **Transport: ***.
  - **Remote Subnet: ***.
  - **Received Interface**: **InsideTLS**.
  - **Signaling Interface**: **OutsideTLS**.
  - **Media Interface**: **OutsideMedia**.
  - **End Point Policy Group**: **SP3_PolicyG**.
  - **Routing Profile**: **SP3_To_SM63**.
  - **Topology Hiding Profile**: **SM63_To_SP3**.
  - Click **Finish**.



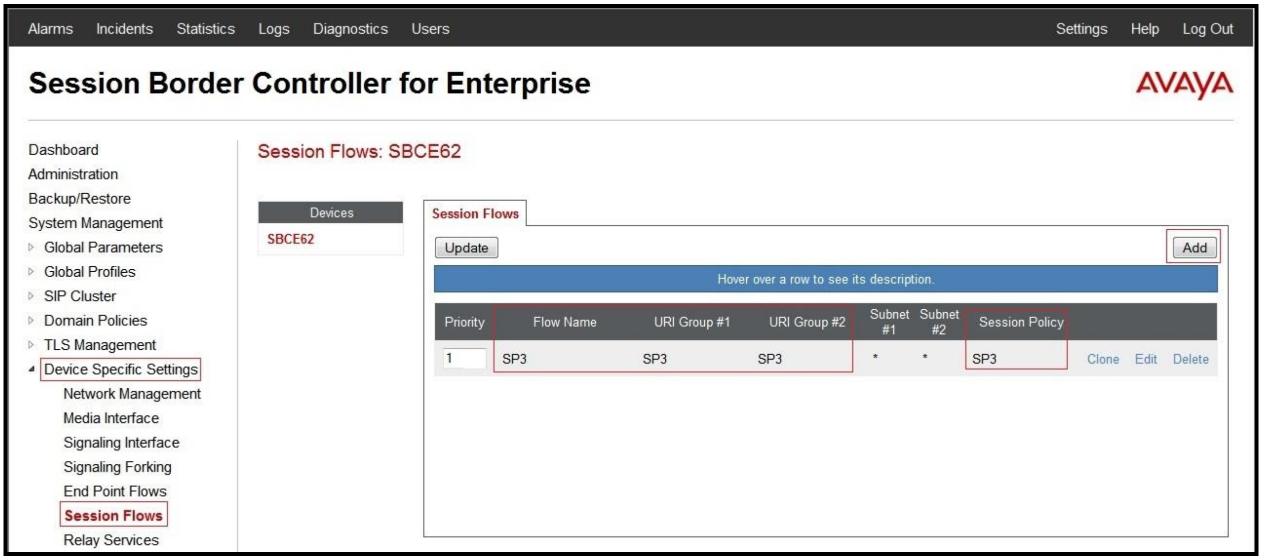
Flow Name: SP3 Flow
Server Configuration: SP3
URI Group: SP3
Transport: *
Remote Subnet: *
Received Interface: InsideTLS
Signaling Interface: OutsideTLS
Media Interface: OutsideMedia
End Point Policy Group: SP3_PolicyG
Routing Profile: SP3_To_SM63
Topology Hiding Profile: SM63_To_SP3
File Transfer Profile: None

Figure 81 - End Point Flow – COLT Server Flow

7.5.5. Create Session Flows

Session Flow determines the media (audio/video) sessions in order to apply the appropriate session policy.

- Select **Device Specific Settings** from the menu on the left-hand side.
- Select the **Session Flows**.
- Select **Add**.
- **Flow Name**: **SP3**.
    - **URI Group#1**: **SP3**.
    - **URI Group#2**: **SP3**.
    - **Session Policy**: **SP3**.
- Select **Finish** (not shown).



Priority	Flow Name	URI Group #1	URI Group #2	Subnet #1	Subnet #2	Session Policy			
1	SP3	SP3	SP3	*	*	SP3	Clone	Edit	Delete

Figure 82 – Session Flows

8. COLT SIP Trunking Configuration

COLT is responsible for the network configuration of the COLT SIP Trunking service. COLT will require that the customer provide the public IP address used to reach the Avaya SBCE public interface at the edge of the enterprise. COLT will provide the IP address of the COLT SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete configurations for Communication Manager, Session Manager, and the Avaya SBCE discussed in the previous sections.

The configuration between COLT and the enterprise is a static IP address configuration.

9. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands that can be used to troubleshoot the solution.

Verification Steps:

1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Troubleshooting:

1. Enter the following commands using Communication Manager System Access Terminal (SAT) interface:
    - **list trace station** <extension number> - Traces calls to and from a specific station.
    - **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.
    - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
    - **status trunk-group** <trunk-group number> - Displays trunk-group state information.
    - **status signaling-group** <signaling-group number> - Displays signaling-group state information.
2. Session Manager:
    - **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.
    - **traceSM -x** – Session Manager command line tool for traffic analysis. Log into the Session Manager management interface to run this command.
3. Avaya SBCE: Debug logging can be started in two different ways:
    - **GUI** of the SBC: **Device Specific Settings → Troubleshooting → Debugging**.
        - SIP only: enable LOG_SUB_SIPCC subsystem under SSYNDI process.
        - CALL PROCESSING: enable all subsystems under SSYNDI process.
        - PPM: enable all subsystems under CONFIG_PROXY process.
    - **Command Line Interface: /tmp/traceSBC**. The tool updates the database directly based on which trace mode is selected.
        - The first option is recommended when traceSBC is used off-line. These debugs can be enabled by the customers through the GUI, they can send the log files, and traceSBC can parse them off-line.
        - The second option is recommended for live captures. When the tool starts, it checks the database to see if debug logging is already enabled. If yes, the tool automatically starts processing the files.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise to COLT SIP Trunking. This solution successfully passed compliance testing via the Avaya DevConnect Program. Please refer to **Section 2.2** for any exceptions or workarounds.

11. References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya, including the following, is available at: http://support.avaya.com/

Avaya Aura® Session Manager/System Manager

[1] *Administering Avaya Aura® Session Manager, Release 6.3, Issue 2, June 2013*
[2] *Maintaining and Troubleshooting Avaya Aura® Session Manager, Release 6.3, Issue 2, May 2013*
[3] *Administering Avaya Aura® System Manager, Release 6.3, Issue 2, May 2013*

Avaya Aura® Communication Manager

[4] *Administering Avaya Aura® Communication Manager, Document ID 03-300509, Release 6.3, Issue 8, May 2013*
[5] *Programming Call Vectoring Features in Avaya Aura® Call Center Elite, Release 6.3, Issue 1, May 2013*

Avaya one-X® IP Phones

[6] *Avaya one-X® Deskphone SIP 9621G/9641G User Guide for 9600 Series IP Telephones, Document ID 16-603596, Issue 1, August 2012*
[7] *Avaya one-X® Deskphone H.323 9608 and 9611G User Guide, Document ID 16-603593, Issue 3, February 2012*
[8] *Avaya one-X® Deskphone SIP for 9640/9640G IP Telephone User Guide, Document ID 16-602403, June 2013*
[9] *Avaya one-X® Deskphone H.323 for 9630 and 9630G IP Deskphone User, Document ID 16-300700, June 2013*
[10] *Using Avaya one-X® Communicator Release 6.1, October 2011*
[11] *Using Avaya Flare® Experience for Windows, Document ID 18-604158, Release 1.1, Issue 2, February 2013*

Avaya Aura® Messaging

[12] *Administering Avaya Aura® Messaging 6.2, Issue 2.2, May 2013*
[13] *Implementing Avaya Aura® Messaging 6.2, Issue 2, January 2013*

Avaya Session Border Controller for Enterprise

[14] *Avaya Session Border Controller for Enterprise Overview and Specification,* Issue 2, December 2013

[15] *Administering Avaya Session Border Controller for Enterprise,* Release 6.2, Issue 2, January 2014

IETF (Internet Engineering Task Force) SIP Standards Specifications

[16] *RFC 3261 SIP: Session Initiation Protocol,* http://www.ietf.org/

[17] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals,* http://www.ietf.org/

Product documentation for COLT SIP Trunk may be found at:
http://www.colt.net/uk/en/enterprise/index.htm

12. Appendix B: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the SBCE, **Section 7.3.6**:

```
within session "All"
{
   act on message where %DIRECTION="INBOUND" and
%ENTRY_POINT="AFTER_NETWORK"
        {

         %HEADERS["From"][1].URI.USER.regex_replace("(\00011)","");
         %HEADERS["Contact"][1].URI.USER.regex_replace("(\00011)","");
         %HEADERS["Request_Line"][1].URI.USER.regex_replace("(\+)","");
         %HEADERS["To"][1].URI.USER.regex_replace("(\+)","");

        }
 }
within session "All"
{
   act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
   {

// Remove unwanted Headers

          remove(%HEADERS["Alert-Info"][1]);
          remove(%HEADERS["P-AV-Message-Id"][1]);
          remove(%HEADERS["P-Charging-Vector"][1]);
          remove(%HEADERS["Av-Global-Session-ID"][1]);
          remove(%HEADERS["P-Location"][1]);

   }
}
```

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.